La protection des données

Poullet, Yves

Published in:
Droit constitutionnel et vie privée

Publication date:
2008

Document Version
le PDF de l'éditeur

LA PROTECTION DES DONNÉES : UN NOUVEAU DROIT CONSTITUTIONNEL
Pour une troisième génération de réglementations de protection des données

Yves POULLET *

INTRODUCTION

1. Le donné technologique s'est profondément modifié avec l'apparition de réseaux numériques aux capacités de plus en plus importantes, tous interconnectés et dont l'utilisation, de plus en plus conviviale fondée sur des protocoles de communication universels, s'appuie en outre sur des terminaux dont la nature se diversifie et dont certains se caractérisent par des performances en croissance exponentielle.

Cette (r)évolution technologique est loin d'être close. Ainsi, les technologies "d'intelligence ambiante" ne sont déjà plus un mythe et la nanotechnologie miniaturise les terminaux et en décuple les capacités de fonctionnement. Il s'agit, et c'est le premier temps de la réflexion, d'esquisser les caractéristiques de cette évolution et les risques d'atteinte à la protection des données.

2. Le deuxième temps de notre réflexion analyse les fondements constitutionnels des législations de protection des données : l'article 8 de la Convention européenne des droits de l'homme est indéniablement le point de départ de cette consécration législative. Il importe cependant de montrer, d'une part, comment le concept central de vie privée a pu évoluer dans la jurisprudence strasbourgeoise au profit d'une conception large de la vie privée comme "droit à l'autodétermination" et, d'autre part, comment cette extension a pu dans le cadre de la prise en compte des risques nouveaux suscités par le développement des technologies et au-delà de la société informationnelle amener la reconnaissance d'un droit à la protection des données nominatives. Ainsi est justifiée ce que nous considérons,

* Professeur aux Facultés de droit de Namur et Liège, Directeur du Centre de recherche informatique et droit (Belgique). yves.poullet@fundp.ac.be http://www.crid.be.

après la première génération exprimée par l'article 8 de la Convention européenne des droits de l'homme et fondée sur la vie privée, comme la deuxième génération des législations vie privée. Cette deuxième génération s'incarne tant dans la Convention n° 108 du Conseil de l'Europe que dans la directive européenne 1995/46/CE de protection des données à caractère personnel. Cette réflexion nous amène à poser la question du besoin de consacrer le droit à la protection des données à caractère personnel comme un nouveau droit constitutionnel à côté de celui traditionnel à la protection de la vie privée, ce que n'hésite pas à proposer la Charte européenne des libertés et droits fondamentaux proposée à Nice, dès 2000.

3. Le dernier chapitre ou acte cherche à montrer l'insuffisance de l'approche traditionnelle des réglementations de seconde génération, c'est-à-dire les législations de protection des données. La thèse est que les nouveaux risques et défis posés par les technologies de l'Internet et de l'intelligence ambiante justifient d'aller au-delà des textes de cette seconde génération, si l'on veut en tout cas que soit assuré le droit à l'autodétermination. Ces nouvelles réglementations, même si les approches traditionnelles restent fondées et pleinement nécessaires, doivent -et la directive 2002/58/CE relative à la protection des données dans le secteur des communications électroniques ouvre la voie- prendre en compte comme tel le fait technologique de la société de l'information à la fois l'infrastructure et les terminaux et les acteurs qui gèrent ou produisent de tels infrastructures et terminaux. C'est sur cette base que seront proposés *in fine* quelques principes qui permettent la pleine maîtrise par l'individu de cet environnement technologique nouveau. Ces principes devraient inspirer la nouvelle génération de réglementations que nous appelons de nos vœux.

ACTE PREMIER
OÙ IL EST AFFIRMÉ LA PROFONDE VULNÉRABILITÉ DE L'INDIVIDU DU FAIT DE L'ÉVOLUTION DU DONNÉ TECHNOLOGIQUE ?

I. LA GLOBALISATION DE L'INFRASTRUCTURE ET DES SYSTÈMES D'INFORMATION

4. Le donné technologique se caractérise par ce qu'il est convenu d'appeler la "globalisation". Sans doute, ce mot évoque-t-il aujourd'hui d'abord l'absence de frontières. Le monde est, grâce aux réseaux, devenu sans frontières. Mon *curriculum vitae* porté sur Internet est accessible depuis les quatre coins de la planète. Les traces conscientes voire inconscientes que génère l'utilisation de mon ordinateur, circulent *via* les réseaux et peuvent être collectées, traitées en de multiples endroits lointains, connus ou inconnus de la personne concernée.

Mais la globalisation peut avoir un autre sens.

5. L'utilisation des réseaux jusqu'il y a peu réservée à des usages professionnels et à partir d'un point fixe rythme désormais notre vie quotidienne. Se multiplient les usages humains ayant recours à ces réseaux (lire un journal, commander un bien ou un service, regarder la TV, louer une vidéo cassette, chercher de l'information, placer ou lire une petite annonce, consulter son compte en banque, effectuer un paiement non liquide, ...) et les réseaux mobiles permettront demain à notre frigo de commander la boisson qui vient à manquer, au propriétaire de surveiller de son lieu de vacances ce qui se passe chez lui, à la maman de vérifier en ligne la température du bébé laissé à la crèche et de vérifier le respect par le personnel de la crèche des horaires des repas ... "Les applications RFID[1] sont plus impressionnantes encore comme en témoignent les premières expériences d'intelligence ambiante"[2] menées par certaines grandes surfaces ou les discothèques[3].

Les développements issus des recherches en nanotechnologies[4] devraient conduire à aller plus loin encore. Ainsi, le corps lui-même pourrait être doté de molécules qui, dotées de propriétés électriques ou chimiques par-

---

[1] Pour un historique des *RFID*, voir : http*://www.rfidjournal.com/article/ articleview/1338/1/129* et les questions vie privée liées à ces applications nouvelles, S. E. SARMA, S. A. WEIS and D. W. ENGELS, *"RFID Systems and Security and privacy Implications"*, Auto-Id Center MIT, Cambridge, disponible sur *http://www.autoidcenter.org.*

[2] "L'environnement d'intelligence ambiante sera capable de reconnaître et de réagir à la présence d'individus et fonctionnera de manière fluide et imperceptible, voire souvent totalement non transparente ...", IPTS, "sécurité et respect de la vie privée du citoyen à l'heure du numérique après le 11 septembre", document de synthèse, juillet 2003, disponible sur le site de la Commission : *http://europa. eu.int/comm/justice_home/fsj/privacy/*

[3] A suivre le cas Baja Beach Club, discothèque barcelonaise où le contrôle d'entrée, le calcul des consommations et les déplacements des membres du club sont contrôlés par un système de RFID fonctionnant grâce à un implant Verichips (*http://www.bajabeach.es*).

[4] Sur la "nanotechnologie" et ses progrès, on consultera pour la définition : *http://www.techweb.com/encyclopedia.*

ticulières, pourraient fonctionner comme un terminal susceptible d'agir au sein du corps et de transmettre des informations sur le fonctionnement de nos organes[5]. L'Homme ainsi est saisi par les TIC non seulement dans son action ou ses attributs externes mais au plus profond de lui.

6. Cette globalisation, entendue cette fois comme le développement d'outils de surveillance de toutes les activités de l'individu est permise par l'évolution à la fois des supports, des terminaux et des réseaux. Quelques réflexions à ce triple propos nous permettent de souligner les risques nouveaux encourus par la personne en matière de protection des données.

II. LES SUPPORTS D'INFORMATION

7. La première évolution concerne les supports d'information. Il est coutumier à leur propos de rappeler la loi de MOORE qui établit que la performance des supports d'information double tous les dix-huit mois (soit par mille tous les quinze ans) alors que, dans le même temps, le prix diminue de moitié pour une performance égale. Dans une étude pour le Conseil de l'Europe[6], nous concluions : "il est devenu et il deviendra de plus en plus possible et de moins en moins cher d'enregistrer la vie de tous les individus de la planète (la nôtre et celle des autres ...)".

A titre d'illustration, nous pouvons examiner la faisabilité de l'enregistrement de toutes les communications téléphoniques sortant d'Europe vers le monde entier. Ce n'est pas rien puisqu'il s'agit de stocker l'équivalent de cinquante milliards de minutes de télécommunications

[5] A cet égard, le projet de loi annoncé aux États-Unis qui viserait à implanter dans le corps de chaque citoyen américain un RFID qui permettrait de connaître les données essentielles de santé en cas d'intervention d'urgence. Les capsules RFID seraient liées à une base de données informatisée créée par le département (= ministère) de la santé des USA afin de stocker et de contrôler les registres de santé de la nation. Cela pourrait être le précurseur d'un projet semblable au Royaume-Uni. *http://www.pcinpact.com/actu/news/RFID_projet_de_loi_un_implant_pour_chaque_citoyen.htm. Cf.* également, l'annonce récente de Microsoft de breveter un système qui rendrait le corps humain, émetteur et récepteur de certaines informations utilisables par des systèmes d'information.

[6] Y. POULLET et J. M. DINANT, "*L'autodétermination informationnelle à l'ère de l'Internet*", Eléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD), Rapport publié sur le site du Conseil de l'Europe, *http://www.coe.int/T/F/Affaires %5Fjuridiques/Coop %E9ration %5Fjuridique/Protection %5Fdes %5Fdonn %E9es/.*

vocales[7] sur une base annuelle[8]. Si l'on considère qu'il faut environ dix mille bits par seconde pour digitaliser la voix et que l'on peut comprimer les données d'un facteur deux (ce qui est classique), on observe qu'il faudra en moyenne de l'ordre de cinq tera octets pour stocker 24 heures de trafic, ce qui à l'heure actuelle est tout à fait envisageable avec des systèmes de *disk array* où chaque disque peut stocker de l'ordre de 400 gigabytes[9]. En outre, le débit moyen de ce flux continu de centaines de milliers de communications simultanées représente un débit d'environ 0,5 gigabits par seconde, ce qui est largement supportable par une seule fibre optique de l'épaisseur d'un cheveu[10]. En d'autres termes, il serait techniquement possible de faire passer TOUT ce trafic téléphonique à travers un mince tube en verre de quelques microns d'épaisseur.

Dans le commerce, on trouve actuellement des systèmes de type walkman capables d'enregistrer le contenu de l'équivalent de plusieurs centaines de CD-ROM classiques au format MP3. Les appareils photos digitaux permettent de stocker des centaines voire des milliers de photos alors que la capacité du film classique plafonne à 36 vues.

Le Registre National de la Belgique qui contient la démographie de tous les belges de la naissance à leur mort ainsi que leurs mariages, professions et adresses successives[11], sans compter des données relatives aux étrangers résidants en Belgique, tiendrait aujourd'hui sans problème sur une cassette DAT de la taille d'une grosse boîte d'allumettes ou sur quelques DVD. Il pourrait intégralement être transmis par fibre optique en quelques dizaines de secondes.

Si cette révolution multiplie les risques d'atteinte à la protection des données, nous soulignons que le principal risque résulte du fait de la miniaturisation des supports et la difficulté de contrôler effectivement l'existence de tels traitements.

[7] Calcul réalisé sur base d'une extrapolation des chiffres fournis par l'Union Internationale des Télécommunications pour l'année 1999 (vu sur : *http://www.itu.int/ITU-D/ict/statistics/atglance/Eurostat 2001.pdf*).

[8] En 1980, cela eut nécessité au bas mot des millions d'enregistreurs avec autant de bandes magnétiques. A cette époque, il fallait un enregistreur pour enregistrer une conversation.

[9] Voir, par exemple sur www.hitachi.com le 400GB Deskstar 7K400.

[10] Actuellement, des débits de 2,5 à 10 gigabits par seconde sont classiques sur ce type de support.

[11] Soit environ 2 milliards d'octets.

III. LES ÉQUIPEMENTS TERMINAUX

8. Une deuxième évolution notable affecte les équipements terminaux. L'évolution est multiple. Elle est bien évidemment technique, d'ordre fonctionnel, ensuite et concerne leur réglementation, enfin.

La notion de "terminal" est définie par la directive européenne sur les équipements terminaux[12] de la façon suivante : "un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications (à savoir des réseaux de télécommunications servant entièrement ou en partie à la fourniture de services de télécommunications accessibles au public)".

Cette définition très large permet d'englober non seulement les ordinateurs personnels, les terminaux classiques comme le téléphone (mobile ou non), le fax ou autres mais également les RFID (Radio Frequency Identifiers)[13], les cartes à puces[14] et demain, les molécules "intelligentes" implantées au sein même du corps des individus. Ce qui caractérise les RFID dont le marché se développe à une allure exponentielle[15] est tant

[12] Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *JOCE* n° L 091 du 7 avril 1999, pp. 10-28.

[13] Ces terminaux que sont les RFID possèdent les éléments suivants :

- un processeur ;
- une mémoire morte ;
- une antenne qui permet tout à la fois de communiquer avec un terminal et de recevoir l'énergie requise pour faire fonctionner l'ordinateur ;
- absence de périphériques d'entrée/sortie accessibles à un être humain ;
- très haut degré de miniaturisation (de l'ordre de quelques millimètres, antenne incluse) Sur les RFID, le lecteur consultera le site très complet : *http://www.rfida.com/nb/identity.htm.*

[14] Certaines cartes à puces sont équipées de processeurs aussi puissants que les célèbres Apple du début des années 80.

[15] Le marché des RFID's se déploie à une échelle mondiale pour identifier et tracer la plupart des biens matériels. On a cité comme cas les chemises Beneton ou les rasoirs Gilette. Les arguments généralement avancés sont la lutte contre le vol en magasin et un environnement ambiant plus intelligent qui permettraient aux objets même les plus insignifiants de communiquer avec leur utilisateur. Une autre utilisation possible est constituée par le numéro de série qui pourrait être gravé dans cette puce scellée dans l'objet.

A.I.D.C., Volume XVII, Droit constitutionnel et vie privée, Tunis 2008

AIDC, VOLUME XVII, Droit constitutionnel et vie privée, Tunis 2007

leur miniaturisation, que le fait qu'ils s'attachent et identifient la possession d'un objet même si indirectement elle révèle le comportement de son possesseur, soulevant la question de savoir si nos législations relatives à la protection des données "identifiant" des personnes sont applicables[16].

9. Au-delà de ce premier phénomène, on souligne deux autres points majeurs relatifs à l'évolution des terminaux.

Ainsi, premier point, la nature de l'équipement terminal : la technologie est passée de l'électromécanique à une électronique programmable. En d'autres termes, le fonctionnement de l'équipement terminal est dicté par un déterminisme qui est celui non de l'utilisateur[17] mais du concepteur de l'appareil voire de tiers qui peuvent insérer dans le terminal des applicatifs permettant une utilisation à distance de ce terminal (ainsi les spywares ou l'ensemble des logiciels de mise à jour de programmes installés

Le système de codification des RFID est révélateur de son ambition. Le code EAN (European Article Number) se compose de 96 bits dont les 36 derniers sont réservés pour le seul numéro de série de l'article. Il s'agit donc de permettre l'identification individuelle de 16 milliards d'objets identiques (du même type et produits par la même firme). Si on ne voit pas quelle entreprise pourrait produire 16 milliards de produits identiques ni l'utilité de différencier le cas échéant ces milliards d'objets identiques, on notera qu'il s'agit de l'ordre de grandeur de la taille prévisible de la population mondiale dans les décennies à venir.

[16] Cette question est largement débattue dans l'opinion du groupe dit de l'article 29 dans le Working document on Data Protection Issues to RFID Technology, en date du 19 janvier 2005, disponible sur : *http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105.en.pdf* qui reprend le considérant 26 de la directive pour conclure que dans la plupart des cas les données créées par les émissions d'un RFID sont des données à caractère personnel. A notre avis, un tel raisonnement est contestable dans la mesure où la recherche de l'identité de la personne n'est pas nécessaire pour pouvoir agir vis-à-vis d'elle et qu'on peut dès lors difficilement parler à propos de données relatives à un objet de données à caractère personnel. Par ailleurs, l'exercice de certains droits qui découlent de l'application de la directive s'avère difficile. A noter que des associations comme CASPIAN aux États-Unis proposent une réglementation des RFID en tant que tels (à cet égard voir le site http ://www.spychips.com/press-releases/right-to-know-bill.html. *Cf.* également, l'avis "aspects éthiques des implants TIC dans le corps humain" du Groupe européen d'Ethique des Sciences et des Nouvelles Technologies : *http://europa.eu.int/comm/european_group_ethics/docs/avis20fr.pdf.*

[17] A propos de la parfaite transparence et maîtrise du fonctionnement des anciens terminaux comme le téléphone ou le fax, lire Y. POULLET, J.-M. DINANT, *"L'autodétermination informationnelle à l'ère de l'Internet"*, Rapport pour le Conseil de l'Europe, nov. 2004, déjà cité.

sur l'ordinateur)[18]. Bref, l'utilisateur d'un terminal n'a qu'une maîtrise partielle de l'ordinateur, sans que l'utilisateur ne soit à l'initiative de ces flux.

Cette absence de maîtrise par l'utilisateur se double par une perte totale par l'État de tout contrôle des normes de production des équipements terminaux. Là où le fonctionnement du terminal "téléphone classique" était sévèrement réglementé, ce n'est plus le cas en ce qui concerne les normes techniques et fonctionnelles qui président au développement de la micro-informatique[19].

10. Une seconde caractéristique est la "multifonctionnalité" présente dans la plupart des équipements terminaux (micro-ordinateurs mais également les nouvelles générations de GSM). La traditionnelle répartition des médias en fonction de leur capacité fonctionnelle (téléphone = transport de la voix ; télévision = transport de l'image et du son, ...) disparaît grâce à la numérisation de tout contenu[20] au profit d'une convergence qui permet à un terminal de fonctionner pour de multiples usages et, dès lors, autorise certains acteurs comme les fournisseurs d'accès ou toute personne intervenant dans le routage voire dans l'aide à la sélection des sites de croiser désormais des données nées de l'utilisation de ces diverses fonctionnalités (ainsi, le téléphone, l'écoute de programmes radio, l'envoi de correspondance, le suivi de programmes de télévision, ...).

IV. LES RÉSEAUX DE COMMUNICATION

11. Cette polyvalence des terminaux s'explique par la polyvalence des réseaux de communication, capables de véhiculer des débits de plus en plus importants, ce qui permet de transmettre en temps réel des contenus de plus en plus riches comme le multimédia[21]. Une autre caractéristique de l'évolution des réseaux est sans doute le progrès rapide de la transmission sans fil qui permet la mobilité des terminaux et la continuité de leur connexion. Enfin, on souligne que la normalisation des protocoles de connexion des terminaux aux réseaux de communications électroniques échappe aux gouvernements[22].

12. Le fait que la communication sur les réseaux modernes de communication s'opère non plus par commutation de circuits mais par paquets a des conséquences non négligeables en matière de protection des données. En d'autres termes, l'information, préalablement numérisée, est envoyée sous forme de nombreux paquets de petite taille (typiquement de quelques dizaines de bits à quelques centaines). En fait, la commutation par paquet permet en général une utilisation optimale de la bande passante et donc de la capacité du support de télécommunication. Cette manière de faire permet un partage extrêmement souple d'un seul support de

AIDC, VOLUME XVII, *Droit constitutionnel et vie privée*, Tunis 2007

[18] Sur le fonctionnement de ces logiciels intrusifs, lire *http://www.clubic.com/actualite-21463-phishing-et-spyware-les-menaces-pesantes-de-2005.html*

[19] Les organes de normalisation et de standardisation en matière de technologie de l'information et de la communication sont de plus en plus des organes privés échappant au contrôle des organisations publiques.

[20] Ainsi, les normes : JPEG pour les photos ; EFR pour la voix ; MPEG pour les images en mouvements, permettent la normalisation de tout signal audio ou images.

[21] En l'état actuel de l'art, la fibre optique, insensible aux parasites électromagnétiques, permet des débits de l'ordre de 10 Gbits/seconde. Les câbles actuels contiennent plusieurs fibres (de quelques dizaines à quelques centaines). Grâce à la technologie DSL, il est aujourd'hui classique d'atteindre des débits allant jusqu'à quatre mégabits/seconde sans devoir modifier le fil téléphonique classique à paire torsadée et avec un appareillage de quelques dizaines d'Euros. Ceci signifie qu'à terme, il est techniquement possible que la télévision emprunte la voie de l'Internet plutôt que celle du satellite ou de la télédistribution par câble coaxial dédicacé. Des expériences en ce sens sont d'ailleurs en cours dans de nombreux pays. Ceci présente un nouvel enjeu. Actuellement, le satellite et le câble de télédistribution, techniquement, ne permettent pas ou peu à l'émetteur de programme de savoir quels sont les programmes regardés par le consommateur (techniquement, tous les signaux arrivent sur l'équipement terminal de l'abonné et c'est celui-ci qui choisit celui qu'il veut regarder). Avec la télévision sur Internet, il sera possible de savoir sur une base individuelle qui regarde quoi et même d'injecter de manière ciblée des publicités à des moments précis, toujours sur une base individuelle.

[22] A propos de l'IETF, le W3C et l'ICANN comme organes de normalisation privés échappant aux réglementations étatiques, lire P. AMBLARD, *Régulation de l'internet,* Thèse, Bruylant, 2004, pp. 70 et s. J. Reidenberg note avec raison que les standards élaborés par ces organisations deviennent une source normative de la conduite des internautes (J. R. REIDENBERG, "Lex informatica : the formulation of Information Policy rules through Technology", 76, *Texas Law Review*, 3 (1998), pp. 556 et s.).

On notera que le protocole IPV6 qui permettra demain d'identifier de manière stable chaque terminal connecté au réseau est discuté au sein de la seule organisation IETF sans que les États ne soient conviés à ce débat. Sur ce protocole, lire : *www.telecom.gouv.fr/documents/ipv6/body.htm* et les réactions du groupe de travail de l'article 29 in avis 2/2002 relatif à l'utilisation d'identifiants uniques dans les terminaux de télécommunication : exemple de l'IPv6, 30 mai 2002, disponible sur le site de la Commission *http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2002_fr.htm*

communication entre des centaines voire des milliers d'utilisateurs simultanés.

Chaque paquet comporte l'adresse de l'expéditeur et l'adresse du destinataire. Sur le réseau, chaque nœud (aiguillage) qui reçoit un paquet sait sur quelle voie envoyer ce paquet sur base de son adresse de destination (on appelle cela le routage). Si, pour une raison ou pour une autre, il ne sait pas envoyer ce paquet, il peut le renvoyer au nœud qui lui a envoyé ce paquet avec une explication.

Une conséquence importante est, en ce qui nous concerne, que le destinataire ou les intermédiaires intervenant dans le transport connaissent ou peuvent connaître le point d'expédition voire l'adresse de l'expéditeur, puisque celle-ci figure sur le paquet qu'il reçoit, et pour les intermédiaires le point d'émission et l'adresse de l'émetteur voire sa localisation. Ce sont les données dites de trafic ou de localisation.

V. LE FONCTIONNEMENT DU WEB

13. Le fonctionnement du web mérite aussi quelques considérations[23]. Afin de mieux interopérer, de dialoguer entre eux, de pouvoir comprendre les messages transmis, le web est devenu sémantique, ce qui veut dire que l'ordinateur lui-même crée des métadonnées à partir de données qu'il stocke ou envoie de manière à ce que, plus facilement, les personnes, voire les ordinateurs, puissent à distance accéder et analyser leur contenu. Les services d'analyse automatique des courriers e-mail sont un bel exemple de cette dimension nouvelle. Sans doute, est-il bon d'insister sur le fait que cette création de métadonnées qui permet de découvrir l'information à partir de mots-clefs et de la conceptualisation, n'est plus nécessairement ni volontaire ni consciente mais le résultat direct de l'ordinateur. Chacun a bien évidemment en tête la fonction des moteurs de recherche comme Google ou le repérage automatique des mots-clés dans nos courriers électroniques développés par la même société.

Une autre évolution est l'utilisation de méthodes d'identification et d'authentification des acteurs du net. Il s'agit à la fois de leur permettre de se faire reconnaître ou connaître chaque fois que l'accès à une ressource, un service ou une information le requiert et, au-delà, de pouvoir les identifier de manière sûre lorsqu'il s'agit de retrouver, dans des bases de données distribuées dans le réseau et ce, sans limites de frontières, une

[23] Sur cette évolution du fonctionnement du Web lire M. RUNDLE, *Ethical implications of emerging technologies in the Information Society*, UNESCO Publications, 2006.

information à leur propos. On note que ces "digital identities" constituent alors des métadonnées. Enfin, on souligne que ces identités digitales peuvent, avec les technologies de la biométrie (l'iris, l'empreinte des doigts, la voix), s'incarner dans des caractéristiques physiques et corporelles, réduites à leurs représentations en données.

Enfin, le web 2.0 amène chacun à s'"afficher" sur internet et ce à travers les blogs ou des outils comme "My Space" ou autres, oubliant sans doute que l'image de soi ainsi placée sur le Net permet à autrui bien souvent inconnu à utiliser cette image et prendre vis-à-vis de vous des décisions qui peuvent conduire à l'exclusion de tel emploi ou de tel service.

14. La miniaturisation des équipements terminaux entraîne l'apparition de nouvelles technologies dites d'"intelligence ambiante"[24]. Ces technologies permettent de connecter directement la personne au monde qui l'entoure, les lieux et les objets et constituent un nouveau défi pour la protection de la vie privée. Sans doute, faut-il d'abord évoquer à cet égard, les nombreux services de localisation spatiale qui offrent une aide au destinataire spécifique au lieu où il se trouve (services de navigation, mais également services relatifs aux caractéristiques de l'environnement).

Les réseaux d'intelligence ambiante ont pour objet de mettre la personne et son environnement directement en interaction. L'intelligence que permettent les TIC et l'accès au cyberespace est dorénavant répartie dans les choses, les lieux, voire nos corps, dans lesquels la technologie se fond pour devenir une seconde nature.[25] Ces technologies de l'intelligence ambiante doivent leur développement à l'extrême miniaturisation des terminaux (*cf.* les RFID[26], terminaux de la taille d'un grain de riz et les

[24] Le terme est utilisé pour la première fois en 1999 par le Groupe consultatif du programme IST de l'Union européenne (l'ISTAG) dans son rapport sur le futur des technologies. Sur tout cela J. AHOLA, "Ambient Intelligence", *ERCIM News*, 2001, n° 47, disponible sur le site : *http://www.ercim.org/publications/Ercim_News/enw47. Cf.* également l'expression "d'Ubiquitous Computing" lancée dès 1991 par M. WEISER, "The computer for the 21st Century", *Scientific American*, 265 (3), pp. 66 à 75.

[25] Selon la vision prophétique de WEISER (cité note précédente) qui, en 1991, affirmait : "les technologies les plus profondes sont celles qui disparaissent. Elles pénètrent dans la vie quotidienne à tel point qu'elles ne s'en distinguent plus. Elles sont invisibles".

[26] Notre propos se fonde sur les descriptions et réflexions proposées sur cette technologie par D. DARQUENNES et Y. POULLET, "RFID : Quelques réflexions introductives à un débat de société", *RDTI*, janv. 2007, pp. 255 à 285. On distingue en effet trois types de RFID ou tags et ce selon la passivité ou non du dispositif mis en place :

nanotechnologies[27] encore dans l'enfance de la recherche et leur connexion via des capteurs et l'Internet à des systèmes d'information). Il s'agit grâce à ces puces de suivre le parcours d'un consommateur dans un supermarché et grâce au dialogue entre la puce de ce consommateur et celles sur les produits de comptabiliser automatiquement les achats effectués[28]. Il s'agit de lire à distance les passeports, pour un frigo intelligent,

- les tags actifs sont équipés d'une source d'énergie autonome (pile ou capteur solaire) et d'une puce ; ils sont capables de se signaler seuls et/ou d'établir des dialogues plus construits avec le dispositif de lecture qui se contente de recevoir le signal radio émis par un tag ; le coût de ces tags est élevé (20 $) même si leur coût est en diminution constante et leur durée de vie limitée par la batterie ;

- les tags semi-passifs n'initient pas de communication avec le lecteur mais sont quand même équipés de batteries qui permettent à la puce de stocker des valeurs de type physique, comme la température, la pression, ... Ce type de tag est donc en général couplé à des capteurs physiques, constituant des petits détecteurs sans fils pouvant servir à contrôler des facteurs environnementaux (par exemple le contrôle d'une consommation énergétique). Leur coût peut aller de 10 à 100 $ par pièce ;

- les tags passifs, qui sont les plus répandus, sont excités par induction électromagnétique (en l'occurrence par l'onde émise par le lecteur- "forward channel") et émettent en retour selon des fréquences radio bien définies une suite alphanumérique fixe ("backward channel"). Comme ces tags ne renferment aucune batterie, leur durée de vie est illimitée. Leur coût est réduit (de 20 cents à quelques dollars) ; ce coût est fonction de la sophistication de la puce (taille de la mémoire ou capacité d'encryptage).

[27] Sur les nouveaux défis que représente la nanotechnologie, lire L. CAMPBELL, "Nanotechnologies and the U.S. National Plan for Research and Development in Support of Critical Information Protection", *Canadian Journal of Law and Technology*, vol.5, n° 3, novembre 2006.

[28] Le secteur de la distribution et des services a été le premier à envisager des applications RFID d'abord confinées à l'intérieur du périmètre des magasins. Les RFID placées sur les produits facilitent la gestion des stocks (commerce sans stock), le paiement automatique aux caisses dans la mesure où la caisse peut lire sans présentation du produit sur le comptoir les achats effectués et présenter la facture à acquitter, de même que la détection de vols (magasin sans caissière et sans vol). Placés en outre sur le caddie du consommateur ou directement sur la carte shopping de celui-ci, les RFID contribuent à une amélioration du profilage (la liste des achats est automatiquement enregistrée en référence au client identifié grâce à la carte du magasin ou, à défaut, grâce à sa carte de paiement) et rendent même envisageables de nouvelles technologies publicitaires : un écran placé sur le caddie pourrait ainsi rappeler l'achat d'un produit dans le passé, signaler telle ou telle promotion ou suggérer des produits d'accompagnement assortis au produit acheté. Outre tout cela, les tags RFID pourraient aussi permettre de faire varier les prix des produits en fonction d'une série de critères tels que la "fidélité" du consommateur concerné, les caractéristiques climatiques du jour, la date de péremption du produit etc.

A.I.D.C., Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2007

de commander la bière manquante, il s'agit pour un poste de télévision, de repérer automatiquement votre présence et d'envoyer l'image du programme sélectionné automatiquement à l'ordinateur personnel de votre bureau. Les applications sont infinies. Elles permettent de caractériser l'intelligence ambiante comme suit.

15. On parle d'"Ubiquitous computing", d'une technologie de l'ubiquité dans la mesure où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus menus de notre vie quotidienne, nos déplacements, nos hésitations, notre consommation domestique. Cette technologie est ensuite une technologie largement invisible ("calm technology") dans un double sens : elle fonctionne largement d'une manière opaque, invisible (nous ne connaissons pas le circuit d'information derrière le fonctionnement de la puce : qui la lit ? Quand ? Quelles informations ? Pour qui ?), mais également elle apparaît comme le prolongement naturel même de notre action (la porte s'ouvre et l'ordinateur s'allume) mettant les choses à notre service. Enfin, cette technologie est dite "apprenante" ("learning technology"). Ses applications ont souvent en effet pour caractéristique d'adapter leur fonctionnement aux données obtenues par leur utilisation. Ainsi, dans le cas du grand magasin, le système tiendra compte de nos achats successifs pour progressivement mieux nous profiler et nous adresser la publicité appropriée.

Ainsi, les technologies d'intelligence ambiante ont pour conséquence d'associer le virtuel et le réel. Au sein des réseaux créés par le dialogue entre les choses entre elles ou avec l'homme, c'est l'espace réel qui se trouve investi par les TIC. Au sein de ces réseaux, l'homme, *in fine*, peut devenir une "chose" elle-même insérée dans une relation avec d'autres choses qui réagissent à la présence de cette chose. On évoquera enfin les questions liées aux applications dites "médicales" des RFID implantés dans le corps humain qui permettent à distance de connaître le fonctionnement de celui-ci, voire de corriger ce fonctionnement, par exemple remédier à l'existence d'un état de stress ou stimuler la mémoire[29].

[29] En matière de santé, on étudie également l'implant de radio-tags sur les humains (La Société Applied Digital Solutions et sa puce Verichip). Ces solutions peuvent être très utiles pour certaines catégories de patients à risque (Alzheimer ou souffrant de problèmes cardio-vasculaires ou encore de diabète), dans la mesure où on pourrait insérer dans la puce les données médicales dites d'urgence, ce qui permettrait en cas de besoin d'intervention vis-à-vis d'un patient incapable de s'exprimer, de lire à distance la puce et de connaître les contre-indications que

16. Cinquante pour cent des habitués des "Baya Club"[30], une société de gestion de dancings et maisons de jeux situés en Hollande et Espagne, ont accepté de se voir implanter une puce RFID dans le corps. Aux journalistes qui s'inquiétaient de leur acceptation, ceux-ci répondent qu'une telle puce facilite grandement leur passage aux entrées du casino où la lecture de la puce permet de reconnaître comme "bons" clients et, par ailleurs, leur permet de ne pas courir le risque de se voir voler leur portefeuille, inutile dans la mesure où les consommations leur sont directement débitées de leur carte de crédit. Cet exemple - et on pourrait les multiplier - illustre combien les logiques sécuritaires et d'efficacité économique (gain de temps, voire d'argent) expliquent le succès des applications. C'est la puce RFID que le gouvernement américain entendait implanter dans le corps de tout citoyen américain pour qu'en cas d'accident et d'inconscience de ce dernier, on puisse l'identifier et connaître les données médicales d'urgence ou plus récemment l'émotion créée par la découverte de l'implantation d'une puce RFID dans les passeports, implantation "à des fins de sécurité"[31].

révèlent ces données d'urgence. Un récent rapport du Groupe européen d'Ethique de la Santé (Avis du Groupe européen d'Ethique des Sciences et des nouvelles technologies auprès de la Commission européenne, *"Aspects éthiques des implants TIC dans le corps humain"*,16 mars 2005) décrit ainsi nombre d'applications dont l'intérêt pour certaines sur le plan de la santé est évident (ex : la stimulation à distance de la mémoire pour les patients frappés de la maladie d'Alzheimer ou un implant qui placé dans le corps d'un patient à maladie chronique comme le diabète permet de contrôler à distance via le téléphone l'état du patient diabétique voire, dans le cadre d'un RFID interactif, de lui envoyer les impulsions nécessaires à un rétablissement de la situation compromise) mais d'autres soulèvent de graves problèmes de respect de la dignité et de l'autonomie humaine (ex : possibilité d'agir à distance sur l'état de stress). Sur ce débat, voir : "Une question éthique très importante se pose alors : Quid de la liberté des Hommes de demain ?", article publié sur le site : *http://www.pcinpact.com/actu/news/Puce_souscutanee_Modernite_branchitude_et_inquietu.htm.*

[30] *Cf.* le célèbre cas de la discothèque Baja Beach Club implantée aux Pays-Bas et en Espagne (*http://www.baja.nl*).

[31] A cet égard, les conclusions de la Smart Card Alliance du 3 novembre 2006 (disponible sur le site : *http://www.smartcardalliance.org/pages/publications-whti-passport-card*) à propos de l'utilisation de la technologie RFID dans les passeports et la possibilité de lire à distance ceux-ci : "the vicinity read Rfid Technology proposed for the passport card, in combination with its weak cryptographic protection, will feed citizen distrust due to the undeniable observation by some technologies that the citizen's unique reference number could be obtained and used to track the citizen whenever the card is outside of its protective sleeve. This raises serious privacy concerns that will have to be overcome if the program

Ainsi, la sécurité, celle publique mais également celle privée des organisations et des citoyens exige toujours plus la mise sur pied de systèmes de contrôle, de surveillance et d'alerte. La rentabilité économique, au sens le plus large, l'efficacité tout court, viennent comme une justification complémentaire où se rejoignent les préoccupations des administrations et des organisations, d'une part, et les intérêts des consommateurs et des citoyens, intérêts soigneusement mis en évidence par les administrations ou organisations.

CONCLUSIONS DE L'ACTE PREMIER

17. Les conclusions de ce bref survol de l'évolution technologique s'énoncent comme suit : la protection des données ne peut être effective dans les réseaux modernes de communication que dans la mesure où les législations prennent en compte :

- de nouveaux types de données : A ce propos, on évoque l'existence de données liées à la possession d'objets qui, sans révéler l'identité du possesseur permettent cependant de suivre ceux-ci et de les contacter. On mentionne ensuite les données générées du simple fait de la communication qui révèlent le type, la durée, la fréquence d'utilisation des réseaux et surtout les destinataires des communications. Peut-on à leur propos parler de données à caractère personnel, au sens de l'article 2 a) de la directive 1995/46/CE ? La notion d'identité est au cœur de la définition de ce type de données. Sans doute, cette définition est-elle large dans la mesure où comme le rappelle le groupe de l'article 29, à propos des cookies ou des RFID[32], en invoquant le considérant 26, l'"identifiabilité" se conçoit en fonction de "l'ensemble des moyens susceptibles d'être raisonnablement mis en place, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne". Outre que comme le reconnaît le groupe lui-même, cette approche même large de la notion de données à caractère personnel ne permet pas de couvrir tous les cas, elle reste théorique dans la mesure où ceux qui exploitent les données nées des cookies ou des RFID ne cherchent pas à identifier la personne concernée mais

is to be embraced by Americans". Dans le même sens, la Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine Readable Travel Documents) disponible sur le site de la FIDIS (projet de recherche européen) : *http://www.fidis.net/press-events/press-releases/declaration-de-budapest.*

[32] "Working document on data protection issues related to RFID technology", 19 janvier 2005 déjà cité.

simplement à profiler[33] le détenteur d'un terminal pour décider vis-à-vis de lui de certaines actions ;

- des objets nouveaux : on pense en particulier aux terminaux qui se multiplient et envahissent notre vie quotidienne, devenant une seconde nature. Leur fonctionnement échappe à la maîtrise de leur possesseur et certains peuvent être "privaticides". On note la multiplication ces dernières années des appels à intervention réglementaire du groupe de l'article 29. Nous reviendrons sur le contenu de ceux-ci dans la troisième partie ;

- des acteurs nouveaux : à savoir particulièrement ceux qui interviennent dans la connexion au réseau ou dans la transmission des communications.

Le propos de l'acte II est de rappeler les fondements constitutionnels de la protection des données depuis l'article 8 de la Convention européenne des droits de l'homme, d'analyser les raisons qui ont poussé à la rédaction de législations en matière de protection des données à caractère personnel et enfin de s'interroger sur base de la Charte européenne de 2000 sur l'existence d'un droit constitutionnel nouveau.

[33] Cette notion de profilage pourrait conduire à considérer que la recherche de l'identité s'opère alors par référence non à des données administratives (nom, prénom, adresse, etc.) mais par rapport "à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale", comme le permettrait le dernier membre de phrase de l'article 2 a) de la directive. Ainsi, un cookie serait une donnée à caractère personnel lorsque le nombre de données collectées grâce au cookie permettrait de constituer une image suffisamment précise de la personnalité de l'individu, peu importe l'aspect considéré (profil économique, psychologique ou physiologique). Cette piste apparaît plus féconde mais elle se heurte au fait que dans l'esprit de la directive ces profils ne sont pas pris pour eux-mêmes et ne constituent des données à caractère personnel que dans la mesure où ils permettent de découvrir l'identité de la personne concernée.

ACTE II
OÙ IL EST QUESTION DES FONDEMENTS CONSTITUTIONNELS DES LÉGISLATIONS DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET DE L'APPROCHE EUROPÉENNE EN LA MATIÈRE

I. LE CONCEPT DE VIE PRIVÉE À L'ORIGINE DES LOIS DE PROTECTION DES DONNÉES : L'ARTICLE 8 DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME

18. L'histoire de la protection des données prend naissance avec l'article 8 de la Convention européenne des droits de l'homme. La disposition laisse concevoir la vie privée comme le "droit d'être laissé seul"[34], lié au droit à l'intimité des personnes. Celui de ne pas voir révéler des informations liées à sa "sphère privée", qu'elle soit physique : le domicile familial ou qu'elle soit l'expression d'une relation à autrui, le secret de la correspondance[35].

La vie privée apparaît ainsi au départ comme un concept indéfini qui ne peut s'approcher que de manière négative et souple. Il s'agit d'informations certes mais au-delà, d'abord de lieux (le domicile) et de relations d'un type particulier (l'espace familial et la correspondance) dont la révélation à des tiers ou la mise sur la scène publique priveraient l'individu de l'espace suffisant pour pouvoir exprimer et forger sa propre personnalité et exercer ses libertés fondamentales[36]. En d'autres termes, cette première génération de réglementation consacre la vie privée non

[34] Le fameux "Right to be left alone" défendu par S. WARREN et L. BRANDEIS dans leur article fameux : "The right to privacy", 4, *Harvard Law Rev.*, 193 (1890).

[35] A ce propos, la Recommandation 428 (1970) du Comité d'experts du Conseil de l'Europe portant déclaration sur les moyens de communication de masse et les droits de l'homme, *Annales de la Conv.* Vol. 13, 1970, p. 65.

[36] Ainsi, P. DE HERT et S. GUTWIRTH ("Privacy, Data Protection and Law Enforcement, Opacity of the individuals and Transparency of power", *Privacy and Criminal Law,* (E. CLAES, A. DUFF and S. GUTWIRTH (ed.)), Intersentia, Antwerpen-Oxford, 2006, pp. 61et s.) parlent de "droit à l'opacité" (Right to opacity) par opposition au "droit à la participation" qui caractérise la seconde génération de réglementation "vie privée". A noter avec raison, leur plaidoyer pour un retour de ce droit à l'opacité dans nos sociétés modernes dites de l'information.

comme une liberté en soi mais comme le minimum nécessaire à la protection de la dignité humaine et à l'exercice de libertés essentielles. Ce minimum varie et s'approfondit avec le temps. La vie privée est éminemment liée à des considérations culturelles et liée de ce fait à des valeurs changeantes et contingentes[37].

Ainsi, on peut lire sous la plume du tribunal constitutionnel espagnol[38] : "Une exposition prolongée à des niveaux déterminés de bruits qui, objectivement, sont inévitables et insupportables, mérite de tomber sous le coup de la protection du droit à l'intimité personnelle et familiale, dans le cadre du domicile, dans la mesure où ils empêchent ou rendent particulièrement difficile le libre développement de la personnalité ...". La vie privée s'élargit ainsi au "droit à l'épanouissement" dans un environnement sain. Ce droit à l'épanouissement[39] interdit par ailleurs de limiter la vie privée "à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables"[40]

19. La vie privée s'élargit sans cesse. Il s'entend à la fois d'une reconnaissance de l'autonomie individuelle vis-à-vis de l'État mais également vis-à-vis d'autrui. Le recours à la notion devient l'argument mis en avant pour défendre le droit des salariés face à leur employeur, le "droit" à la reconnaissance des couples homosexuels[41] et la légitimité de certaines

[37] Sur cette évolutivité certaine du concept et son caractère essentiel, lire entre autres, L. BURGORGUE-LARSEN, "L'appréhension constitutionnelle de la vie privée en Europe", *in Le droit à la vie privée au sens de la Convention européenne des droits de l' Homme*, F. SUDRE (éd.), Collection Droit et Justice, n° 63, Bruylant, Nemesis, 2005, p. 72.

[38] Tribunal constitutionnel, 24 mai 2001, n° 118/1001. Mêmes réflexions de la Cour européenne des droits de l'homme dans les affaires Guerra et surtout Moreno Gomez (Arrêt du 16 novembre 2004) cette fois à propos d'industries polluantes. Sur ces affaires, J. P. MARGUÉNAUD, "De l'identité à l'épanouissement", *in Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme* déjà cité, pp. 220 et s.

[39] Sur cette évolution, notamment, O de SCHUTTER, "La vie privée entre droit de la personnalité et liberté", *Rev. T.D.H.* (1999), pp. 827 et s.

[40] Arrêt Niemetz c. Allemagne, CEDH. 16 décembre 1992, § 29. Il s'agissait ici des relations de travail. Plus récemment et toujours à propos des relations de travail, on citera l'arrêt Copland.

[41] Voire à la parentalité de ces couples. A cet égard, les discussions parlementaires en Belgique sur l'adoption par les couples homosexuels lors du vote d'une

pratiques sexuelles[42] L'État se voit en outre imposer une obligation positive de contribuer à ce développement de l'autonomie des citoyens tant vis-à-vis de lui même que dans le cadre de relations interindividuelles[43]. Il est coutumier de présenter l'évolution du concept de privacy dans la jurisprudence de la Cour européenne des droits de l'Homme en distinguant deux temps : un premier temps voit dans ce concept l'outil juridique de la protection contre les intrusions, le "Right to be left alone" ou "Right to opacity" et dans un second temps, la "vie privée" est proclamée comme le droit à l'autodétermination, le droit à l'épanouissement individuel. La première conception correspond à une approche négative qui limite la possibilité pour l'État de s'introduire dans le domaine "réservé" considéré d'abord comme physique de l'individu ; la seconde à une approche plus positive qui rend l'État débiteur, à l'égard des individus, des conditions matérielles et psychiques nécessaires à leur épanouissement individuel. Cette seconde conception s'exprime tant dans la maîtrise que l'individu doit avoir de son environnement, de ses relations à autrui, en partie de son identité nominale et physique (le droit au transsexualisme) que de son libre choix dans la manière dont il décide de sa vie avec autrui.

Dans ce contexte d'élargissement progressif, la protection de la vie privée est, en ce sens *hybride :* de "défensive" contre toute ingérence de l'extérieur conçue comme la défense d'un "jardin clos", garant d'un minimum nécessaire à l'épanouissement de l'individu, elle devient "offensive" et se transforme en exigence de reconnaissance par l'État des conditions du libre épanouissement de toutes les libertés individuelles, nécessaires à l'épanouissement de chacun, "y compris de permettre à cet indi-

récente proposition de loi où l'article 8 est largement évoqué comme fondement de ce "droit". (Sur ce point, lire les longs développements du Conseil d'État, développements en écho aux discussions parlementaires sur l'existence d'un droit des couples homosexuels à adopter, droit déduit de l'article 8 de la CEDH repris *in Doc Parl. Ch. rep.*, Sess. 2004-2005, Doc 51-0393/002, pp. 40 et s.

[42] Sur la jurisprudence strasbourgeoise à cet égard, lire G. GONZALEZ, "La liberté sexuelle", *in Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, op. cit.*, pp. 157 et s.

[43] Sur cette obligation positive, lire F. SUDRE, "Rapport introductif", *in, Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, op. cit.*, pp. 25 et s. Cette obligation positive nous paraît suffire à justifier les interventions de l'État prises dans le domaine de la protection de la vie privée dans le cadre de relations interindividuelles sans que l'on ne doive recourir à la théorie doctrinale très controversée de l'effet horizontal de la Convention européenne des droits de l'homme.

vidu de réviser ses propres conceptions de la vie bonne, par l'organisation d'un environnement suffisamment hétérogène et pluraliste pour lui fournir l'occasion d'opérer ces révisions"[44].C'est le sens de concept de "droit à l'autodétermination" (*Selbstbestimmungsrecht)* mis en avant par le tribunal constitutionnel allemand en 1983[45], qui n'est rien d'autre que la consécration d'une liberté, "mais d'une liberté différente par rapport aux autres libertés publiques en ce qu'elle concerne exclusivement chaque individu dans sa subjectivité et sa singularité propres. A ce titre, elle relève aussi des sciences humaines : psychologie, anthropologie, sociologie, philosophie, valeurs éthiques, et touche à la fois au réel, à l'imaginaire et au symbolique qui sous-tendent les comportements des hommes. Ce n'est donc pas un hasard que la Cour européenne des droits de l'homme ait choisi de renoncer explicitement à en définir le contenu, notamment dans ses arrêts Niemetz (1992) et Pretty (2002). Mais c'est moins sans doute par impuissance que pour en ménager un champ d'application quasi-illimitée"[46].

20. Ce soi-disant "droit" à la vie privée auquel il est fait référence ne fonctionne pas comme un droit subjectif mais plutôt comme une prérogative indéterminée que la personne peut faire valoir vis-à-vis de l'État dans la mesure où la Convention a un effet direct sur lui et l'oblige à prendre les garanties idoines à la protection de la vie privée. Tantôt, sa réclamation est judiciaire et amène le tribunal saisi à vérifier au vu des circonstances si l'intérêt avancé par la personne plaignante relève bien de cette "sphère" indispensable à l'épanouissement de l'Homme, en d'autres termes de ses libertés essentielles[47] et, le cas échéant, à vérifier les conditions d'applicabilité de l'article 8.2 qui permet à l'État de faire prévaloir d'autres intérêts. "La "privacy" serait ici simplement ce que l'individu fait de la liberté qui lui est reconnue. Elle n'est pas définissable a priori :

[44] O. DE SCHUTTER, "La vie privée entre droit de la personnalité et vie privée", *Rev. T.D.H.*, 1999, p. 861

[45] BverfG 15 déc. 1983, *BverfGE*, 65, 1, 41. A noter que cette décision concernait précisément la question de la constitutionnalité d'un recensement statistique.

[46] M. T. MEULDERS-KLEIN, "L'irrésistible ascension de la "vie privée" au sein des droits de l'Homme", in Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme, *op. cit.*, p. 308 et les références à nombre d'auteurs, on enverra le lecteur en particulier à l'ouvrage majeur de F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité,* Bruylant, Bruxelles, 1990.

[47] Voir à cet égard, S. GUTWIRTH, "Privacyvrijheid ! De vrijheid om zichzelf te zijn", *Rathenau Instituut*, Den Haag, Juin 1998, pp. 51 et s.

sa portée n'apparaît qu'à travers les conflits que suscite son exercice, c'est-à-dire qu'elle n'est appréhendée par le droit que dans un cadre contextualisé"[48]. Tantôt, le cas échéant, après quelques victoires judiciaires, la réclamation se transporte sur le plan politique et entend voir consacrer législativement des droits subjectifs nouveaux suivant l'obligation positive mise à charge des États de respecter les libertés individuelles progressivement dévoilées à travers le concept de vie privée. Ainsi, la liberté essentielle que représente la vie privée débouche dans la reconnaissance de multiples droits subjectifs nouveaux qui, sans épuiser la notion, en dessine les contours, progressivement et dans un mouvement jamais achevé.

Dans ce débat, il est piquant de constater que la technologie a été le point de départ de cette réflexion[49] même si la disposition de 1950 s'explique par d'autres raisons historiques[50]. On ajoute -et l'exemple de la protection contre les industries polluantes en est un signe marquant- que la technologie a bien souvent été le moteur de l'évolution de la notion et de son extension. Cette réflexion nous conduit à envisager la seconde génération de législation à la fois dans ses liens avec la première génération mais également dans sa rupture avec celle-ci.

II. LES LÉGISLATIONS DE PROTECTION DES DONNÉES AU DELÀ DE LA VIE PRIVÉE AU REGARD DU CONCEPT DE VIE PRIVÉE

A. Des deux facettes de la vie privée

21. Comment situer les législations de protection des données dans ce contexte ? La directive européenne de 1995- mais la convention n° 108 du Conseil de l'Europe l'avait précédée dès 1981- sont indéniablement le fruit de cette évolution de la notion de vie privée. Sans doute, la protec-

[48] C'est par ces mots que de SCHUTTER (*art.cité,* p. 839) résume la position de RIGAUX ("La vie privée. Une liberté parmi les autres !", *Travaux de la faculté de droit de Namur*, Bruxelles, Larcier, 1992, pp. 120 et s.) et celle de GUTWIRTH, *op. cit.*

[49] Comme le note D. SOLOVE (*The Digital person, Technology and privacy in an Information Age*, New York University Press, 2004, pp. 57 et s.). L'article de WARREN et BRANDEIS part de la constatation des risques d'intrusion dans l'intimité des personnes causés par les premiers appareils photographiques portables.

[50] Il est clair que l'article 8 s'explique d'abord par la volonté d'éviter toute reproduction de certains agissements de l'Allemagne nazie.

tion de la vie privée s'y entend par rapport à un risque précis, celui né des traitements de l'information, en particulier aggravé par l'usage des technologies de l'information et de la communication. Le préambule de la Convention n° 108[51] pour la protection des personnes à l'égard du traitement des données à caractère personnel, conclue le 28 janvier 1981 note que cette Convention "vise à étendre la protection des droits et libertés de chacun, notamment le respect du droit à la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés". La Convention dans l'esprit de ses auteurs répond aux menaces que fait peser le changement qualitatif de l'utilisation des données à caractère personnel grâce aux traitements informatisés de celles-ci, en particulier les risques de discrimination. Sans doute, l'évolution des technologies de l'information crée-t-elle un risque d'atteinte à l'intimité sans commune mesure avec celui des méthodes de surveillance envisagées dans les années 1950. On note cependant que la perception des risques liés à ces traitements évolue avec le temps. Et le parallèle avec l'évolution d'une notion défensive de la vie privée à une conception plus agressive déjà notée aide à comprendre cette évolution.

B. Des législations de protection des données et de leur justification : la décision du tribunal constitutionnel allemand de 1983 et sa consécration du droit à l'autodétermination informationnelle

22. Sans doute, les premières législations de protection des données étaient-elles focalisées sur les risques d'atteinte à l'intimité des personnes et sur les dangers d'une surveillance des individus[52]. La référence exclusive à la vie privée et l'importance des données sensibles dans les premières législations traduisent leur filiation avec l'article 8 de la Convention européenne. Cette première conception explique également que la première législation, celle du Land de Hesse en 1970 se soit concentrée sur les seuls traitements d'information opérés par l'État.

Progressivement, il est cependant constaté que les technologies de l'information et de la communication accentuent le déséquilibre

[51] STE n°108. La Convention est entrée en vigueur le 1er octobre 1985.

[52] La loi du Land de Hesse est sans doute un bel exemple de cette approche, de même que la loi française de 1978, prise en réaction au projet SAFARI. Sur cette focalisation des premières législations sur la vie-privée intimité et la nécessité d'élargir le débat, lire entre autres, D. J. SOLOVE, "Conceptualizing Privacy", 90 *California Law Review*, 2002, 1085 et s. ; P. BLOK, "Het recht op privacy", *Boom Juridische uitgevers*, 2003.

d'informations entre les personnes concernées et les responsables des traitements qu'ils soient publics ou privés. Ces technologies menacent dès lors non seulement l'intimité (la vie privée-intimité) mais l'ensemble des libertés individuelles (la vie privée-libertés) ainsi, la liberté d'obtenir un crédit, un logement, celle de se déplacer, etc.[53], mais également des libertés consacrées par d'autres articles de la Convention européenne des droits de l'homme, ainsi la liberté d'expression[54], celle de saisir la justice[55], la liberté de vote, etc. En même temps, elles engendrent un risque important de discrimination en cas d'utilisation de données inexactes ou surtout disproportionnées[56].

23. La décision du tribunal constitutionnel allemand du 15 décembre 1983 dans l'affaire du recensement statistique[57] est sans doute à rappeler ici. Elle ancre le droit à la protection des données, considéré comme l'"*informationnelle Selbstbestimmung*" dans les droits fondamentaux de la dignité humaine et de l'auto-développement, deux droits consacrés par la Constitution allemande (§ 1 et § 2.1), justifie la consécration du droit à la protection des données dans notre société de l'information en même temps qu'elle en décline les éléments essentiels. Le tribunal note que "les possibilités de contrôle et d'exercice d'influence croissent de manière

[53] La protection des données constitue le moyen d'assurer la vie privée et sa consécration est une conséquence directe de l'obligation positive des États d'assurer le respect de la vie privée au sens le plus large.

[54] Qui ne voit que la protection des données est le meilleur garant de la liberté d'expression dans la mesure où le contrôle de l'expression de chacun permis par les technologies modernes de l'information et de la communication peuvent amener les citoyens voire les journalistes à limiter leur expression par peur des conséquences.

[55] On sait la lutte que nombre d'autorités de contrôle en matière de protection des données ont mené contre l'utilisation par des entreprises de renseignements relatifs à l'introduction de recours judiciaires qui leur permettaient de cibler des consommateurs "agressifs" ou des employés "revanchards". De même, l'informatisation du judiciaire et la diffusion des décisions judiciaires font craindre la mise en péril des droits de la défense (A ce sujet D. MOREAU, Y. POULLET, "La justice au risque de la vie privée", *in Phénix et la procédure électronique, Travaux de la CUP*, 02-2006, Vol. 85, pp. 87 à 141.

[56] A ce propos, le principe repris dans toutes les législations de protection des données suivant lequel les données doivent être pertinentes, adéquates et non excessives par rapport aux finalités légitimes poursuivies par le responsable du traitement.

[57] Voir arrêt du Tribunal constitutionnel fédéral allemand, *Volkszählungsgesetz, BVerfGE 65, 1*, du 15 décembre 1983.

exponentielle et inconnue jusqu'à ce jour. Ces possibilités peuvent influencer le comportement humain par la pression psychologique exercée tant par les pouvoirs publics que privés. Dans les conditions actuelles de traitement de l'information, l'autodétermination individuelle présuppose que les individus se sentent libres de choisir quant aux actions à prendre. Si quelqu'un s'avère incapable de pouvoir prédire quelles informations à propos de lui sont connues et à qui elles peuvent être transmises, il est inhibé de manière cruciale dans sa liberté de planifier ou de décision libre. Ceci n'aura pas seulement pour conséquence de nuire à ses chances de développement mais aura aussi un impact sur le bien public dans la mesure où l'autodétermination est une condition élémentaire d'une société libre et démocratique basée sur la capacité de chaque citoyen d'agir selon son propre vouloir et de coopérer avec autrui". Le tribunal ajoute : "Considérant les dangers énoncés ci-dessus et liés aux traitements automatiques de données, le législateur plus qu'auparavant est tenu de mettre en place les sauvegardes institutionnelles et procédurales qui permettront de répondre aux dangers d'atteinte aux droits de la personnalité" et il met en avant les principes de légitimité et de proportionnalité d'une part, de transparence d'autre part.

24. En d'autres termes, le tribunal :

- considère que l'informatisation de nos sociétés crée de nouveaux risques au regard de la vie privée conçue comme droit à l'autodétermination tant par l'opacité des traitements qu'elle génère, par le déséquilibre qu'elle crée entre ceux qui ont l'information et les personnes concernées que par les possibilités de discrimination que cette puissance de l'information peut entraîner. Pour être plus précis, le risque essentiel identifié par le Tribunal constitutionnel allemand dès 1983 est celui du "conformisme anticipatif", la volonté des citoyens de se conformer à la norme de comportement, à laquelle explicitement ou implicitement les autorités privées ou publiques se réfèrent par la logique des traitements qu'elles mettent en place. Ce "conformisme anticipatif" va à l'encontre de la construction identitaire de chacun, nécessaire pour assurer la démocratie. Le second risque relevé par la Cour vise ce qu'on peut qualifier de "réductionisme", le fait que les traitements manipulent des données, c'est-à-dire des images partielles des personnes et dès lors ont tendance à ne plus apercevoir la personne qu'à travers leurs données et à agir selon celles-ci, fussent t-elles déformantes, partielles voire erronées au regard de la réalité ;

- souligne le double rôle de la vie privée dans la société de l'information, d'une part, le rôle de garantie de l'individu contre la tyrannie de la majo-

rité[58] et, d'autre part, son rôle essentiel d'appui à la démocratie dans la mesure où la capacité d'un développement identitaire permet à l'individu de participer effectivement et de manière originale à la délibération démocratique en lui réservant un espace dans lequel il peut se forger une opinion à l'abri des pressions de l'opinion. En ce sens, la vie privée est un bien public essentiel à la démocratie et à l'exercice de toutes les autres libertés. Ainsi, il est évident que la possibilité d'une expression libre renvoie à notre capacité d'autodétermination, à ce sentiment de non-surveillance et de non-opacité des traitements qui concernent les données qui résultent de notre prise de parole ou y sont contenues. Oserais-je signer une pétition en faveur de telle cause généreuse si je crains que, demain, un moteur de recherche puissant offre à un futur potentiel employeur les moyens de me stigmatiser pour cette prise de position ?

[58] A propos de la tyrannie de la majorité, ce merveilleux passage de A. de TOCQUEVILLE (La démocratie en Amérique, 1835) : "Un roi (...) n'a qu'une puissance matérielle qui agit sur les actions et ne saurait atteindre les volontés ; mais la majorité est revêtue d'une force tout à la fois matérielle et morale, qui agit sur la volonté autant que sur les actions, et qui empêche en même temps de fait, et le désir de faire".

"En Amérique, la majorité trace un cercle formidable autour de la pensée. Au-dedans de ces limites, l'écrivain est libre ; mais, malheur à lui s'il ose en sortir. Ce n'est pas qu'il ait à craindre un autodafé, mais il est en bute à des dégoûts de tous genres et à des persécutions de tous les jours. La carrière politique lui est fermée : il a offensé la seule puissance qui ait la faculté de l'ouvrir. On lui refuse tout, jusqu'à la gloire".

"Les princes avaient pour ainsi dire matérialisé la violence ; les républiques démocratiques de nos jours l'ont rendue tout aussi intellectuelle que la volonté humaine qu'elle veut contraindre. Sous le gouvernement absolu d'un seul, le despotisme, pour arriver à l'âme, frappait grossièrement le corps ; et l'âme, échappant à ces coups, s'élevait glorieuse au-dessus de lui ; mais dans les républiques démocratiques, ce n'est point ainsi que procède la tyrannie ; elle laisse le corps et va droit à l'âme. Le maître n'y dit plus : Vous penserez comme moi, ou vous mourrez ; il dit : Vous êtes libre de ne point penser ainsi que moi ; votre vie, vos biens, tout vous reste ; mais de ce jour vous êtes un étranger parmi nous. Vous garderez vos privilèges à la cité, mais ils vous deviendront inutiles ; car si vous briguez le choix de vos concitoyens, ils ne vous l'accorderont point, et si vous ne demandez que leur estime, ils feindront encore de vous la refuser. Vous resterez parmi les hommes, mais vous perdrez vos droits à l'humanité. Quand vous vous approcherez de vos semblables, ils vous fuiront comme un être impur et ceux qui croient à votre innocence, ceux-là mêmes vous abandonneront, car on les fuirait à leur tour. Allez-en paix, je vous laisse la vie, mais je vous la laisse pire que la mort".

- le droit à la protection des données doit être reconnu par l'État comme une condition nécessaire au vu des nouveaux risques rencontrés par les libertés dans la société de l'information. Il traduit une dimension nouvelle du droit à la protection de la vie privée considéré comme droit à l'autodétermination et à la dignité et donc droit fondamental, fondamental vis-à-vis de tous les autres droits fondamentaux ;

- il ne s'agit pas pour le Tribunal constitutionnel allemand de consacrer la vie privée comme un droit de propriété de l'individu sur ses données : "Les individus, affirme la Cour allemande, ne possèdent pas dans un sens absolu la maîtrise de leurs données à caractère personnel. Notre personnalité se développe et dépend de la communication au sein de communautés sociales. L'information même basée sur un individu reflète cette dimension sociale et ne peut être associée au seul individu. Notre Constitution résout le conflit entre l'individu et la société en faveur d'un individu se référant à la ou à des communauté(s) et fondamentalement lié à celle(s)-ci".

C. La jurisprudence de l'article 8 de la Convention européenne des droits de l'homme et la protection des données

25. La prise en compte des risques nouveaux qu'encourent nos libertés du fait de l'informatisation de nos sociétés s'est faite progressivement. C'est avec beaucoup de réticence que les juges de Strasbourg ont relayé cette préoccupation nouvelle à travers une interprétation hardie de l'article 8 de la Convention européenne des droits de l'homme. On note que l'interprétation traditionnelle de l'article 8 s'avérait insuffisante à englober la réalité nouvelle des traitements de données, comme en témoigne la jurisprudence de la Cour fondée sur cet article, du moins jusque 1999 et l'affaire Rotaru.

À propos des contrôles d'identité impliquant l'enregistrement des données figurant sur la carte d'identité, la Commission européenne des droits de l'homme dans sa décision du 9 septembre 1992[59] avait jugé que de telles données ne constituaient pas des données relevant de la vie privée. De même, à propos de données collectées par caméra de vidéosurveillance dans le cadre d'une manifestation publique ou plus largement dans un espace public au motif que la personne se trouvant dans un tel espace

[59] Commission Européenne D. H., 9 septembre 1992, Req. n° 16810/90 F. Reyntjens c. Belgique, DR, 73, p. 136.

ne pouvait espérer aucune confidentialité de ses faits et gestes[60]. Ainsi l'article 8 ne protégeait que les données obtenues en violation de la vie privée de la personne c'est-à-dire dans un cadre intime ou lorsque la personne concernée avait souhaité protéger les données la concernant de toute divulgation. L'arrêt Leander c. Suède prononcé par la CEDH le 26 mars 1987 constituait un premier pas dans la direction d'une protection des données à caractère personnel encore que dans l'hypothèse il s'agissait de données très sensibles relatives à la personne, recueillies par la police, en l'occurrence sur le passé communiste d'une personne qui devait être engagée sur une base navale de l'armée et que ce qui est reproché à la police est plus l'absence de transparence du traitement de telles données jugées secrètes par la police, que le fait qu'il s'agissait de données à caractère personnel[61]. Seule, répète la Commission encore en 1988 dans l'affaire Hilton c. Royaume Uni, constitue une ingérence dans la vie privée l'utilisation par des services policiers d'informations touchant à la sphère de la vie privée[62]. La même assertion est présente dans une décision de la Commission européenne des droits de l'homme le 14 janvier de la même année et ce, à propos d'images prises lors d'une manifestation publique[63].

26. Il a fallu donc attendre l'arrêt Rotaru c. Roumanie prononcé le 4 mai 2000[64] pour que les juges de la Cour européenne des droits de l'homme considèrent que l'article 8 de la Convention européenne des droits de l'homme englobe les garanties de la Convention n° 108 du 28 janvier 1981. En l'occurrence, le gouvernement roumain se voyait reprocher une décision prise sur base d'informations touchant au passé communiste de

[60] Commission Européenne D. H., 12 oct. 1973, X c. Royaume Uni, Req. n° 5877/72, Ann. Conv., 16, p. 328. Dans le même sens, Commission Européenne D. H., 7 décembre 1992, Req. n° 18395/91, non publiée mais citée par K. ROGGE, "The Protection of Private Life and Technological challenges", *Bull D. H.*, n°2 (1994), p. 23.

[61] "Le registre secret de la police renfermait sans contredit des données relatives à la vie privée de Mr Leander. Tant leur mémorisation que leur communication, assorties du refus d'accorder à Mr leander la faculté de les réfuter, portaient atteinte à son droit au respect de la vie privée, garanti par l'article 8§1".

[62] Commission Européenne D. H., 6 juillet 1988, Req. n° 12015/86, DR, 57, p. 128.

[63] Commission Européenne D. H., 4 janvier 1988, Herbecq c. Royaume de Belgique, Req. n° 32200/96 et n° 32201/96, *JTDE,* 1998, p. 67.

[64] Cour Européenne D. H., 4 mai 2000, *Rev. T. D. H.*, n° 45, (2001), p. 127 et s., note O. DE SCHUTTER, "Vie privée et protection de l'individu vis-à-vis du traitement de données à caractère personnel".

la personne concernée. Le gouvernement arguait que de telles données étaient de notoriété publique et sortaient donc du champ protégé par l'article 8 de la Convention européenne des droits de l'homme. A cet argument, la Cour répond : "le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables. De surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de "vie privée"(arrêt Niemetz et Halford)". Elle souligne ensuite "la concordance entre cette interprétation extensive et celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 ... dont le but est de garantir ...à toute personne physique ... le respect ... notamment de son droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel la concernant, ces dernières étant définies ... comme "toute information concernant une personne physique identifiée ou identifiable". En outre, ajoute la Cour, des données de nature publique peuvent relever de la vie privée lorsqu'elles sont de manière systématique recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne".

D. La Convention n° 108 du Conseil de l'Europe et la reconnaissance de droits nouveaux

27. Le mérite de la Convention n° 108 est incontestablement d'élargir le débat dans deux directions : la première est d'instituer en vue de la protection des données à caractère personnel certaines restrictions à l'utilisation de celles-ci, de créer des obligations de sécurité et administratives à charge de ceux qui traitent des données à caractère personnel et de restreindre, d'une part, la liberté des responsables de traitements, entreprises ou associations, en particulier leur liberté d'entreprendre ou d'associations et, d'autre part, les prérogatives d'intérêt général de l'État. En outre, ces lois confèrent aux personnes concernées de véritables droits subjectifs, selon la définition d'un tel droit c'est-à-dire, selon la thèse récente de Mr LEONARD, "un pouvoir juridique spécifique reconnu par le droit objectif à son titulaire sur la chose ou la prestation qui en forme l'objet en vue de la satisfaction de ses intérêts et pour lequel il reçoit du droit objectif, le pouvoir d'imposer son respect aux tiers au moyen, si

AIDC-VOLUME XVII, Droit constitutionnel et vie privée, Tunis 2007

nécessaire, d'une action en justice spécifique"[65]. Ainsi, sont reconnus le droit à l'information, le droit d'accès, de rectification, etc.

Ces droits subjectifs permettent à la personne concernée de maîtriser la circulation de son image informationnelle et d'apprécier les raisons de son utilisation. Cette connaissance lui permettra de faire valoir devant le juge ou l'autorité de protection des données ses libertés[66] et d'opposer celles-ci aux libertés ou à l'intérêt qui fondent le traitement opéré par le responsable du traitement.

On conçoit à cet égard le rôle central joué par l'autorité de protection des données dans ce débat entre libertés ou entre libertés et intérêt général. Il s'agit à l'occasion d'un traitement particulier, de mettre en balance les intérêts et libertés mis en cause d'une part et poursuivis d'autre part, afin de déterminer lesquels ou lesquelles doivent prévaloir. Cette mise en balance peut conduire à une remise en cause de l'existence même du traitement ou de manière plus limitée de son contenu.

28. La Convention n° 108 et plus encore la directive de 1995 ne sont plus à proprement parler centrées sur la vie privée, conçue de manière défensive, c'est-à-dire comme un noyau dur de données sensibles aptes à protéger l'intimité de la personne concernée ou ses relations de correspondance privée mais, de manière plus élargie, comme la condition indispensable des libertés essentielles de l'individu. C'est désormais tout traitement de données à caractère personnel qui est apprécié à l'aune de l'ensemble des libertés individuelles et publiques de même qu'à la lutte contre toute forme de discrimination.

Ces textes consacrent donc un élargissement de la préoccupation initiale. Ils instaurent des droits subjectifs de protection en faveur de la personne concernée[67] et conçoivent le débat de la protection des données dans le contexte d'une relation de pouvoirs entre, d'une part, les responsables du

---

[65] Th. LEONARD, *Conflits entre droits subjectifs, libertés civiles et intérêts légitimes*, Thèse, Namur, Larcier, 2005, p. 105.

[66] ... que le même auteur définit comme : "*le pouvoir d'agir ou de ne pas agir attribué par le droit objectif à chacun en vue de la satisfaction des intérêts qui en forment le but et pour lequel il reçoit du droit objectif les moyens juridiques de défense vis-à-vis des tiers*" (*op. cit.*, p. 288).

[67] Sur cette notion de "droits subjectifs de protection" (auxquels la personne protégée ne peut renoncer) distingués des droits subjectifs de disposition (qui constituent des droits de libre disposition pour ceux auxquels ils sont attribués), lire X. DIJON, *Le sujet du droit en son corps. Une mise à l'épreuve du droit subjectif*, Thèse, Larcier, 1982.

traitement et, d'autre part, les personnes concernées. Ainsi, la protection des données est progressivement instituée comme une garantie fondamentale nécessaire pour assurer dans une société de l'information le respect de l'ensemble des libertés tant individuelles que publiques et pour lutter contre tout risque de discrimination. Il s'agit d'offrir à l'individu une certaine maîtrise de son environnement informationnel et dès lors de la circulation de son image en même temps que de limiter les activités de traitement de l'information mises en place par les responsables de traitement tantôt, pour les personnes privées, au nom de leur liberté d'entreprendre ou d'association, tantôt, pour l'État, au nom de l'intérêt général. Les réglementations de protection des données sont à considérer comme une conséquence de la consécration de la protection de la vie privée, conçue d'abord au sens étroit mais elles ont progressivement débordé ce cadre pour assumer un rôle vis-à-vis de l'ensemble des libertés consacrées par la Convention européenne des droits de l'homme.

II. VERS LA CONSÉCRATION D'UN DROIT CONSTITUTIONNEL AUTONOME EN MATIÈRE DE PROTECTION DES DONNÉES ?
LES ARTICLES 7 ET 8 DE LA CHARTE EUROPÉENNE DES LIBERTÉS ET DROITS FONDAMENTAUX ET LES CARACTÉRISTIQUES DE L'APPROCHE EUROPÉENNE

A. Vers un droit constitutionnel autonome ?

29. Que penser dès lors de la Charte européenne des droits fondamentaux[68] qui distingue en ses articles 7 et 8[69] deux concepts : vie privée et protection des données qui, certes, se complètent et se recoupent mais dont l'extension n'est pas semblable. L'article 7 évoque, dans l'esprit de la jurisprudence traditionnelle de la Convention de 1950, le respect de la vie privée et familiale du domicile et des communications.

Il énonce : "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications".

[68] *JOCE*, 2000, C 364/10, 18 décembre 2000. Sur cette charte, lire K. LEENAERTS et E. DESMUTTER, "Een "Bill of Rights" voor de Europese Unie", *in Bydragen aan een Europese Grondwet*, Staats rechtsconferentie, 2000, pp. 107-138.

[69] Ces articles de la charte sont intégralement repris dans le projet de Constitution européenne aux articles II 67 et II 68.

L'article 8 crée un droit nouveau[70] : le droit à la protection des données à caractère personnel, qu'il distingue du droit à la vie privée.

"1. Toute personne a droit à la protection des données à caractère personnel la concernant".

"2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en exiger la rectification".

"3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante".

Ainsi, l'article 8 étend la protection à toutes les données à caractère personnel, épingle les limitations au traitement en même temps qu'il consacre les droits subjectifs essentiels de la personne concernée et souligne le rôle de l'autorité indépendante dans le contrôle du respect de ces règles. Cette consécration quasi constitutionnelle[71] de la protection des données comme un principe distinct de celui de la vie privée doit être soulignée. Sans doute, la protection des données s'enracine-t-elle historiquement dans la protection de la vie privée au sens de la Convention européenne des droits de l'homme, sans doute, certains traitements constituent-ils des violations de notre droit à l'intimité et à notre droit à l'épanouissement mais la réglementation instaurée par cette seconde génération déborde ce cadre étroit et vise d'office en réglementant leur mise en œuvre et leur contenu tout traitement de données à caractère personnel, qu'il y ait ou non atteinte à la vie privée mais de manière à prévenir de telles atteintes.

30. Ceci dit que l'on se comprenne bien : la protection des données si elle consacre des droits subjectifs nouveaux trouve bien son fondement dans les préoccupations qui sont à la base de la notion de vie privée. Il s'agit bien au travers de ce droit nouveau de continuer à affirmer la nécessité de reconnaître à chacun une capacité d'autodétermination, ce qui est l'essence même de la reconnaissance du droit à la vie privée, conçue

[70] Sur ce droit nouveau, Recommandation 4/99 du groupe dit de l'article 29 sur l'inclusion du droit fondamental à la protection des données dans les droits fondamentaux européens, 7 septembre 1999 disponible sur le site de l'Union européenne : *http://www.ec.europa/justice_home/fs.privacy.html.*

[71] Sur la valeur quasi constitutionnelle de la Charte, lire entre autres les commentaires de D. PISSOORT et P. DE HERT (ed.), "Vie privée et données à caractère personnel", *Politeia*, 2004, Titre 1, pp. 20 et s. (mise à jour décembre 2004).

comme condition structurante de notre démocratie comme l'affirme le tribunal constitutionnel allemand et se déclinant en deux facettes inséparables : d'une part, le droit à l'intimité ou plus largement le droit de se retirer de la société et d'autre part, celui d'y développer ses propres choix. Ces deux acceptions de la notion de privacy ne sont pas incompatibles entre elles, bien au contraire. Elles traduisent un objectif commun : permettre à l'individu de participer pleinement à la vie sociale. La réalisation de cet objectif suppose, à la fois, le "droit à la séclusion" ou plutôt la liberté de ne pas être exposé (le "droit" de ne pas participer à la société de l'information), condition structurelle de l'évolution de l'Homme dans la mesure où elle permet l'autonomie réflexive et la liberté de définir et partant de choisir son mode d'existence et de relation à autrui et, à la fois, le "droit à participer pleinement à une société démocratique de l'information en contrôlant la circulation de son image informationnelle et ses usages". On note que ces deux acceptions sont intimement liées et s'arc boutent l'une à l'autre : la première est condition de la seconde dans la mesure où elle permet à l'individu de construire son autonomie et son identité afin dans un second temps, de s'affirmer dans la société (la privacy comme condition de la liberté d'expression) et de veiller au respect de ses libertés par une maîtrise des flux informationnels qui l'entourent (contrôle du pouvoir informationnel d'autrui) afin notamment que soit garanti son droit à la séclusion (effet retour de la seconde acception sur la première : je ne peux participer que si on me garantit une opacité partielle, condition de ma liberté).

31. En conclusion il importe de ne pas oublier cette filiation de la protection des données à caractère personnel sous peine de figer le texte et de ne plus apercevoir les fondements même de cette protection qui permettra au fur et à mesure où l'évolution de notre société de l'information se développe grâce aux technologies nouvelles épinglées dans la première partie de l'exposé et présente de nouveaux risques pour l'autodétermination des personnes de faire évoluer cette protection au-delà des limites actuellement proposées par nos législations, ce qui sera précisément l'objet de notre Acte III.

B. Les caractéristiques de l'approche européenne

32. Il serait utile d'approfondir les caractéristiques de cette approche européenne et tout d'abord de répondre à la question suivante : Quelle pourrait être la conséquence d'une consécration constitutionnelle du "droit" à la protection des données, comme droit de l'homme, distingué dorénavant du "droit" à la vie privée ? On sait que l'article 8 de la Convention euro-

péenne des droits de l'homme, malgré la jurisprudence hardie de la Cour, ne vise que les seuls traitements des données opérés par le secteur public[72]. La reconnaissance aurait pour effet d'élargir son champ d'intervention et de rendre plus visible ce droit aux yeux des citoyens Par ailleurs, ces derniers pourraient dès lors baser leur action directement sur base de ce droit sans devoir le fonder sur la violation d'une disposition législative possible[73]. Enfin, la consécration de ce "droit" permet de l'asseoir comme valeur à l'égal des autres libertés constitutionnelles, en particulier la liberté d'expression lorsque ces libertés entrent en conflit[74].

---

[72] A cet égard, les réflexions de L. BYGRAEVE, "Data protection pursuant to the right to privacy in human rights treaty", *Int. Journ. of Law and Technology*, 6, n° 3, pp. 247 et s. ou d'O. DE SCHUTTER, "Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel, observations sous l'arrêt Rotaru", *Rev. T. D. H.*, 2001, pp. 180 et s.

[73] Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, WP. 26, Recommandation 4/99 concernant l'inclusion du droit fondamental à la protection des données dans le catalogue européen des droits fondamentaux, 7 septembre 1999 : "Le groupe, qui réunit les autorités chargées de la protection des données dans les États membres de l'Union européenne, approuve pleinement l'initiative du Conseil européen visant à l'élaboration d'une charte communautaire des droits fondamentaux. Elle fait observer que certains pays européens ont inscrit dans leur constitution un droit fondamental à la protection des données. Dans d'autres pays, ce droit a acquis un statut constitutionnel au travers de la jurisprudence.

Dans leurs décisions et leurs arrêts, la Commission européenne et la Cour européenne des droits de l'homme ont défini et précisé un droit fondamental en se basant sur différents droits de l'homme liés à la protection des données à caractère personnel.

Enfin, le nouvel article 286 du traité sur l'Union européenne dispose que les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel sont applicables, à partir du 1er janvier 1999, aux institutions et organes de l'Union européenne. L'intégration de la protection des données à caractère personnel dans les droits fondamentaux européens rendrait cette protection applicable dans l'ensemble de l'Union et mettrait en évidence l'importance croissante de la protection des données dans la société de l'information."

[74] A noter sur ce point, déjà l'article 9 de la directive qui vise à concilier ces deux valeurs constitutionnelles : "Les États membres prévoient, pour les traitements à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations ... dans la mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression."

33. Au delà, relevons la caractéristique essentielle de l'approche européenne. Les données à caractère personnel ne constituent pas de simples valeurs marchandes, elles sont régies par des règles de droit public dont le but est en définitive la protection des libertés et, de manière plus essentielle encore, de la dignité humaine qui ne peut survivre que si est assurée à chaque personne une maîtrise suffisante de son environnement afin qu'il puisse exprimer ces choix, la relation de la personne avec ces données nominatives ne peut donc s'assimiler à une relation de propriété mais doit tenir compte des limites imposées par le fait qu'au-delà de toute information nominative, il est question de libertés et d'une conception du respect dû à la dignité de l'individu considérée comme personne[75]. Ainsi, curieusement, les législations de protection des données ne consacrent pas une maîtrise totale de l'individu sur "son" information. "La liberté qui découle de la dignité humaine n'est pas une liberté robinsonienne", comme le note Meulders-Klein[76] à la suite des commentateurs de la Constitution allemande qui consacre le droit à l'autodétermination[77]. Cette affirmation explique l'originalité de l'approche européenne par rapport à celle américaine[78]. Elle se traduit en particulier premièrement par la nécessité d'un examen de la légitimité de tout traitement des données ; deuxièmement, par le rôle du consentement, condition nécessaire mais non suffisante de la légitimité d'un traitement ; troisièmement, par l'importance de l'autorité de contrôle quatrièmement par le rôle certain

[75] Sur cette relation fondamentale entre vie privée et dignité umaine, lire J. H. REICHMANN, "The right to privacy", *in Philosophical Dimensions of Privacy*, F. D. SCHOEMAN (ed.), 1984, p. 272.

[76] M. T. MEULDERS-KLEIN, art. cité, p. 314 et les références citées.

[77] L'article 2.1 de la Constitution consacre le "droit de chacun au libre épanouissement de sa personnalité", ce droit doit être lu en référence à l'article 1.1 qui affirme "la dignité intangible de l'être humain comme principe universel".

[78] On notera que tous les auteurs américains ne partagent pas ce que nous qualifions un peu rapidement comme étant l'approche américaine. Ainsi, on note les remarques de SCHWARTZ ("Beyond Code for Internet Privacy : Cyberspace Filters, Privacy control, and Fair Information Practice", *Wisconsin Law Rev.*, 2000, p.787.) : "In place of Lessig's idea that privacy protects a right of individual control, this Article has developed a concept of constitutive privacy. Information Privacy is a constitutive value tat safeguards participation and association in a free society. Rather than simply seeking to allow more and more individual control of personal data, we should view the normative function of information privacy as inhering in its relation to participatory democracy and individual self determination. Information Privacy rules should carry out a constitutive function by normally defining multidimensional information territories tat insulate personal data from the observation of different parties".

mais limité de l'autorégulation. Dans le cadre de cet article, nous ne pouvons développer longuement ces quatre caractéristiques de l'approche européenne. Nous nous bornerons à quelques considérations sur ces différents points.

34. L'examen de la légitimité[79] des traitements de données à caractère personnel auquel l'article 6 de la directive européenne contraint chaque responsable de traitement introduit l'obligation de procéder à un examen de proportionnalité entre les intérêts poursuivis par le responsable du traitement et ceux de la personne concernée. Cet examen s'opère sous contrôle a priori ou a posteriori de l'autorité de contrôle même si l'article 7 de la directive instaure certaines présomptions de respect de cette légitimité ainsi, le consentement indubitable de la personne concernée, l'exécution d'un contrat et la réalisation d'un intérêt légitime du responsable du traitement ou d'un tiers à qui communication est faite, supérieur à l'intérêt de la personne concernée. Cette exigence de légitimité qui exige le contrôle social et ne permet pas de considérer le traitement des données à caractère personnel comme le résultat de décisions purement privées distingue l'approche américaine et des principes de l'OCDE de l'approche européenne[80]. Ce principe de légitimité est fondamental. Il implique la nécessité de prévenir tout contrôle excessif des personnes concernées et d'en assurer le caractère loyal[81].

35. L'exigence de finalité légitime renvoie à une réflexion sur le "consentement" comme fondement de la légitimité de certains traitements opérés dans le cadre de l'utilisation par la personne concernée des services de l'Internet. Comme on le sait, même si l'article 5 se borne à mentionner le principe général de légitimité, le consentement est cité par les autorités de protection des données, la Directive européenne (article 5.1) et par la doctrine comme première base de légitimation d'un traitement. Dans la mesure où les réseaux modernes sont interactifs, le consentement peut

[79] T. LEONARD et Y. POULLET, "Les libertés comme fondement de la protection des doness nominatives", *in* F. RIGAUX, *La vie privée : une liberté parmi les autres* ?, Travaux de la Faculté de Droit de Namur, n°17, Larcier, 1992, pp. 250 et ss. ; S. GUTWIRTH, "De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijk levensfeer ten opzichte van de verwerking van persoonsgegevens", *T.P.R.*, 1993, 1409 et ss.

[80] Les principes américains du "Safe Harbor", pourtant reconnus comme adéquats par la Commission par sa décision 2000/520 CE, (*JOCE.*, 25 août 2000, L 215, 7-47) ne contiennent pas de référence à ce principe.

[81] A cet égard, lire les commentaires de BYGRAEVE ("Data Protection Law : Approaching its rational, logic and limits", *Den Haag, Kluwer Law In.t, 2002.)*

plus facilement être réclamé comme fondement de légitimité des traitements et être préféré à d'autres fondements plus traditionnels comme la balance d'intérêts. La facilité pour le maître du fichier d'obtenir le consentement de la personne concernée explique que certaines législations n'hésitent pas à réclamer dorénavant le consentement pour légitimer certains traitements, ainsi, la directive 2002/58 de l'Union européenne, à propos des traitements des données de trafic, de localisation[82].

Cette considération amène certains à considérer dès lors que le consentement peut suffire pour légitimer un traitement. A cet égard, on rappelle que le développement par le World Wide Web Consortium (W.3.C.) de la Platform for Privacy Preferences (P.3.P.)[83] reposait également sur la possibilité pour l'internaute de négocier avec le fournisseur de services qui ne répondait pas à ses Privacy Preferences et d'aboutir alors à un accord qui serve de fondement légitime au traitement considéré. Même si cette négociation n'a jamais été déployée sur une grande échelle, notamment par le biais d'agents électroniques, P3P reste révélateur de la volonté de l'industrie de se donner les moyens de négocier avec la personne concernée l'utilisation qui pourrait être faite de ses données. La protection de la vie privée pourrait ainsi, dans une certaine mesure, se négocier[84]. Il nous paraît cependant que le consentement ne peut constituer une base suffisante de légitimité[85]. Il nous paraît que dans certains cas, la légitimité

[82] On mentionnera également le système de l'opt-in choisi pour régler la question de l'envoi de courrier non sollicité. Un autre argument en faveur de l'opt in est le caractère intrusif de l'envoi qui pénètre directement le domicile virtuel de la personne concernée, la facilité d'envoi de tels messages et l'absence de tout coût pour l'émetteur.

[83] Outre l'opinion émise par le groupe de l'article 29 (Opinion 11/98 du Groupe européen de protection des données, groupe dit de l'article 29 à propos de la Platform for Privacy Preferences (P3P) et des Open Profiling Standards (OPS), opinion disponible à *http ://europa.eu.int/comm/dg15/fr/media/dataprot/wpdoes /wp11.fr.pdf*, lire sur ce protocole, J. CATLETT, "Technical Standards and Privacy : An open Letter to P3P Developers", disponible à l'adresse : *http:// www.junkblusters.com/standards.html.*

[84] Sur la contractualisation du traitement des données ainsi opérée par la technologie, lire P. M. SCHWARTZ, "Beyond Lessig's Code for Internet Privacy : Cyberspace, Filters, Privacy control and Fair Information Practices", *Wisconsin Law Review*, 2000, pp. 749 et s. ; M. ROTENBERG, "What Larry doesn't Get the Truth", *Stan. Techn. L. Rev.*, 2001, 1, disponible sur le site : *http://www. sth.Stanford.edu/STLR/Articles/01_STLR_1.*

[85] A noter à cet égard la rédaction maladroite de l'article 7 de la Charte européenne des droits fondamentaux qui met sur le même pied le consentement et les autres fondements légitimes prévus par la loi alors que l'article 7 de la directive

d'un traitement même appuyé par un consentement spécifique, informé et libre peut se voir remis en cause. Trois raisons militent en ce sens :

- le consentement même loyalement obtenu ne peut légitimer certains traitements contraires à la dignité humaine ou à d'autres valeurs essentielles à laquelle un individu ne peut renoncer ;

- les individus consommateurs doivent être protégés contre des pratiques où en échange d'avantages économiques, leur consentement est sollicité ;

- la question de la protection de la vie privée n'est pas une simple affaire privée mais met en jeu des considérations d'ordre social et exige une possibilité d'intervention et un contrôle marginal par les autorités publiques[86] ;

- enfin la doctrine du consentement comme fondement suffisant du traitement des données ne prend en compte ni la question des "capabilitiés"[87] dans la société de l'information, le fait que les nécessités ou avantages liés à la vente de données peuvent être attractifs pour des personnes fragiles socio-économiquement parlant, ni la théorie des dominos qui met en évidence le fait que la divulgation volontaire par une personne de "ses" données personnelles "force" les autres à donner la même information, sous peine de suspicions envers eux. L'interdiction de "renoncer" à la protection de la vie privée et de divulguer, dans certains contextes à tout le moins, "ses" informations à caractère personnel, se justifie moins par une approche paternaliste de protection des individus contre les choix déraisonnables qu'ils pourraient faire, que par un souci de protection d'un idéal d'égalité entre les citoyens. Comme le suggère Margaret Jane Radin, la renonciation aux droits fondamentaux consentie par certains (qu'ils se sentent "contraints" à cette renonciation pour des raisons socio-économiques, ou qu'ils réalisent que cette renonciation leur confère un avantage comparatif par rapport aux autres individus se trouvant en concurrence avec eux sur le même "marché" de l'emploi, de l'assurance ou de tout autre bien social) annihile la liberté de choix des autres, dans la mesure où leur renonciation génère un sentiment général d'obligation et

95/46 CE entrevoit le consentement comme une des conditions de légitimité nécessaire certes mais non suffisante.

[86] A ce propos, les réflexions de SCHWARTZ, article cité note 63.

[87] Voir Amartya SEN, *Inequality Reexamined*, Harvard University Press, 1995.

une "marchandisation" de l'information privée forçant tout un chacun à entrer sur ce nouveau marché de l'information à caractère personnel [88].

36. La place de l'autorité de contrôle est fondamentale dans la reconnaissance du droit à la protection des données. Sa création est une exigence de longue date de la jurisprudence strasbourgeoise en matière de protection de la vie privée[89]. La directive européenne lui accorde une importance toute particulière tant au niveau national[90] qu'au niveau européen[91] et dans le cadre des flux transfrontières[92].

[88] Margaret Jane RADIN, "Justice and the Market Domain", *in* John CHAPMAN, J. Roland PENNOCK, *Markets and Justice*, New York University Press, 1989, p. 168 : "the domino theory asserts that market evaluations of objects and activities are imperialistic, diving out other and better ways of perceiving and evaluating objects and activities. Once some individuals attach a price at a given object, relation or activity, they and others tend to lose their capacity to perceive or evaluate that object, relation or activity as anything but a commodity with a specific market price. Moreover, the theory asserts, once certain objects or activities are commodified, there is a tendency for other objects or activities of the same sort or even of other sorts also to be seen and evaluated merely in terms of their actual or potential market value". Pour une exploration plus détaillée de ce thème voir Antoinette Rouvroy, "Information génétique et assurance. Discussion critique autour de la position "prohibitionniste" du législateur belge", *J.T.*, n° 5978, 2000, 585-603 et Antoinette ROUVROY, *Human Genes and Neoliberal Governance : A Foucauldian Critique*, Routledge-Cavendish, 2007, (Chapter 7 : A critical assessment of economic and actuarial perspectives on genetics and insurance).

[89] *Cf.* en particulier l'arrêt Gaskin v. United Kingdom ((1989) Serie A, n° 160) où la Cour reproche sévèrement à l'État britannique de ne pas avoir mis en place de système par lequel un organe indépendant pourrait entendre la personne concernée au cas où son droit d'accès lui serait refusé.

[90] *Cf.* Article 28 de la directive "Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application sur son territoire des dispositions ... de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies".

[91] L'article 29 de la directive institue le "Groupe de protection des données à l'égard du traitement des données à caractère personnel" qui "a un caractère consultatif et indépendant". On souligne l'originalité de cette création au niveau européen dans la mesure où dans nul autre secteur, une telle institutionnalisation, qui permet à ce groupe de jouer un rôle de lobby au sein même des organes décisionnels européens, n'a été réalisée. On ajoute l'importance du travail réalisé par ce groupe. Sur tout cela, Y. POULLET, *"EU. Data Protection Directive : Ten years after"*, CL&SR, 2006, à paraître).

[92] En particulier, le rapport du groupe de l'article 29 : "Transferts de données à caractère personnel à des pays tiers : application des articles 25 et 26 de la directive européenne relative à la protection des données, doc. adopté le 24 juillet 1998", (W.P. 12) insiste sur la nécessité pour le pays tiers de disposer d'autorités de surveillance et de contrôle pour satisfaire aux exigences d'une protection adéquate. "L'instrument (offert par le pays tiers) doit fournir soutien et assistance aux personnes concernées confrontées à un problème lié au traitement des données personnelles les concernant. Il convient donc de désigner une instance impartiale et indépendante, d'accès facile, chargée de connaître des plaintes émanant de personnes concernées et de statuer sur les infractions au code".

L'autorité de contrôle joue un rôle central dans l'équilibre voulu par les législations européennes entre responsables de traitement et personnes concernées. Il s'agit à la fois grâce à cette autorité de servir de soutien et d'assistance dans les démarches des personnes concernées vis-à-vis des responsables de traitement afin d'assurer l'effectivité de leurs droits subjectifs. Il s'agit ensuite de disposer d'un outil de contrôle et de surveillance du respect de leurs obligations par les responsables de traitement. Enfin, l'autorité de contrôle joue un rôle prospectif vis-à-vis des développements technologiques et des risques potentiels vis-à-vis de la protection des données, conformément au principe de précaution[93].

37. L'article 27 de la directive 95/46/CE invite les États membres et la Commission "à encourager l'élaboration des codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales ...". Ainsi, est promue l'autorégulation qui se doit cependant d'être conforme à la législation voire lui apporter une plus-value tant du point de vue de son contenu que de l'effectivité[94]. Dans le même temps, cette reconnaissance par les textes européens des autres modes de régulation de la protection des données s'accompagne

[93] Sur ce triple rôle, nos réflexions in Y. POULLET, *"Vues de Bruxelles : l'autorité de protection des données"*, *R.F.A.P.*, 1999, pp. 181 et s.

[94] Le cas hollandais où les codes de conduite sectoriels se sont multipliés doit être cité. A cet égard, lire G. OVERKLEEFT, *Verburg, Wet persoonsregistraties : norm, toepassing en evaluatie*, thèse, Tilburg, W.E.J., Tjeenk Wilrijk, 1995. Sur cet apport, ne serait-ce que par la lisibilité plus grande et l'application concrète de principes législatifs vagues à un cas concret, lire C. J. BENNETT et C. D. RAAB, *The Governance of Privacy*, Ashgate, 2003, pp. 122 et 123.

Rien n'est dit par contre en ce qui concerne le besoin d'assurer une certaine légitimité aux codes de conduite ainsi par la nécessité d'une consultation des représentants des catégories des personnes concernées. Cette préoccupation au niveau européen de la légitimité des codes de conduite est exprimée pour la première fois en matière de protection des consommateurs par l'article 16 de la directive 2000/31/CE dite "Commerce électronique" du 8 juin 2000. On note cependant que le recueil des observations des personnes concernées est un élément de la procédure "d'homologation" prévue à l'article 27.2.

d'un contrôle ou tout au moins d'un certain encadrement de ces derniers. A l'occasion de l'homologation des codes de conduite, les autorités de protection des données sont sensibles à un examen serré des conditions de conformité de la protection offerte par l'instrument, aux exigences de la loi de protection des données, à la légitimité de leurs auteurs et, enfin, à l'effectivité plus grande offerte par ces modes de régulation à l'appui de la protection déjà inscrite dans les législations de vie privée.

L'autorégulation, présentée comme le modèle alternatif à la régulation publique, s'avère en effet tentante. Les "Privacy Policy", simples "commitments", "codes of Practices" ou "Privacy Standards"[95] émanant des responsables de traitement, seuls ou encadrés, comme c'est le cas dans les "Safe Harbor Principles"[96] fleurissent. Ils présentent l'avantage pour la personne concernée de développer, dans un langage bien plus convivial que celui de la loi, des principes plus adaptés à la réalité des traitements d'une entreprise ou d'un secteur[97]. Ils reposent sur un engagement consciemment pris par un secteur ou une entreprise. Bref, l'autoréglementation semble avoir l'avantage d'une plus grande effectivité[98].

38. A cet égard cependant, les reproches adressés à l'autorégulation sont connus : le premier est sans doute la question de la légitimité des mul-

[95] Sur la directive entre ces trois types d'autorégulation, C. J. BENNETT et C.D. RAAB, *The gouvernance of Privacy*, Ashgate, 2003, pp. 12 et s.

[96] Cf. à cet égard, la décision 2000/520/CE de la Commission conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la protection assurée par les principes de la sphère de sécurité" et par les questions souvent posées y afférentes, publiées par le ministère du Commerce des États-Unis d'Amérique, *JOCE*, 25 août 2000, L 215, pp. 7 et s. L'encadrement par les pouvoirs publics est assuré par le fait que les "Safe Harbor Principles" ont été négociés avec les pouvoirs publics et que les déclarations de conformité sont publiées sur le site officiel du Department of Commerce. Sur ces "Safe Harbor Principles" comme mode de co-régulation, lire Y. POULLET, "Les "Safe Harbor Principles" ; Une protection adéquate ?", disponible sur : *http://www.droit-technologie.org*.

[97] Sur cette meilleure adaptation de l'autorégulation aux besoins normatifs des protagonistes de la société de l'information, lire P. TRUDEL et *alii*, *Droit du cyberespace*, Thémis, Montréal, 1997, Chap. 3, pp. 12 et s.

[98] Pour un jugement très nuancé sur la situation aux États-Unis de l'effectivité des codes de conduite en matière de protection des données, lire K. JAMAL, M. MAIER et S. SUNDER, *Enforced Standards Versus Evolution by General Acceptance : A comparative Study of E-Commerce Privacy Disclosure and Practice in the U.S and the U.K.*, Joint Center, Working Paper, 3-8 July 2003.

tiples produits de cette auto-réglementation. Comme l'écrit Weber[99], "avec l'autorégulation, tout groupe pertinent n'est pas nécessairement impliqué". Ainsi, on s'inquiète des codes de conduite imposés aux internautes, qu'ils soient simples employés, consommateurs, patients ou lecteurs de journaux sans négociation préalable avec les représentants de ces derniers. Le second reproche est le manque de garantie quant à l'effectivité de ce mode de régulation[100]. Comment s'assurer que les codes contiennent des sanctions lorsque l'urgence d'une commande interdit la lecture détaillée et fastidieuse de cette privacy policy souvent mal structurée et que rien ne garantit qu'un recours aura lieu en cas de non-respect par son émetteur ou qu'il pourra s'armer d'un bras efficace pour obtenir sanction et exécution de celle-ci[101].

L'attitude européenne vis-à-vis de l'autorégulation représente donc un mélange d'accueil et de méfiance, dans la mesure où, comme le rappelait le document "Mieux légiférer" de l'Union européenne[102], les mécanismes de régulation alternatifs ne peuvent être appliqués "si les droits fondamentaux ou des choix politiques importants sont en jeu". C'est aux autorités publiques de fixer les lignes essentielles des protections indispen-

[99] R. H. WEBER, *Regulatory models for the online World*, Zurich, Schulthess, 2002, p. 85. Sur ce même point, A. ROSSNAGEL, "Weltweites Internet-Globale Rechtsordnung", *Multimedia und Recht*, 2002, p. 69 et J. REIDENBERG, "L'instabilité et la concurrence des régimes réglementaires", *in Les incertitudes du droit*, E. MACKAAY (éd.), Montréal, Thémis, 1999, pp. 133 et s. (à noter que l'auteur étend sa critique à la régulation technologique).

[100] A ce propos, les recommandations de la Federal Trade Commission (F.T.C.) qui, en 2000, publiait un rapport (*http://www.ftc.gov/reports/privacy2000/pdf*) sur l'application des principes de "Fair Information" à la protection de la privacy. Cette instance concluait que les efforts d'autorégulation étaient insuffisants dans la pratique et recommandait le vote d'une législation fédérale adéquate, formulée en termes généraux et technologiquement neutre dans le cadre de laquelle l'autorégulation pourrait prendre sa place et obtenir une meilleure effectivité.

[101] Sur tous ces points, lire le rapport très critique de quatre ans d'expérience des "Safe Harbor Principles" fondés précisément sur ce système des "privacy policies", rapport préparé dans le contexte de l'évaluation de la décision de la Commission de 2000 à propos de l'adéquation du système des Safe Harbor, J. DHONT, M. V. PEREZ-ASINARI, Y. POULLET with the collaboration of J. REIDENBERG and L. BYGRAEVE, *Safe Harbour Decision Implementation Study*, at the request of the E.U Commission, publié sur le site web de la Commission : *http://ec.europa.eu/justice_home/fsj/privacy*.

[102] Accord interinstitutionnel publié au *J.O.C.E.*, 31 décembre 2003, C 321/1. Sur cet accord, lire E. DEGRAVE, *J.T.D.E.*, 2007, Octobre

sables à la garantie des libertés des citoyens. Elles veilleront à fixer le cadre protecteur de manière technologiquement neutre et conformément aux principes de subsidiarité[103] et de proportionnalité. Il ne s'agit pas pour elle de trop dire, ni a fortiori de tout dire mais de laisser à d'autres modes de régulation ainsi encadrés le soin de répondre de manière appropriée aux objectifs qu'elle aura fixés et vis-à-vis desquels les pouvoirs privés auteurs des normes techniques ou d'auto-régulation, devront se conformer.

ACTE III
VERS UNE TROISIÈME GÉNÉRATION DE LÉGISLATIONS DE PROTECTION DE LA VIE PRIVÉE : LA DIRECTIVE 2002/58/CE CONTIENT LES ÉLÉMENTS DE BASE D'UNE NOUVELLE APPROCHE DE QUELQUES PRINCIPES NOUVEAUX À METTRE EN VIGUEUR

I. LA DIRECTIVE EUROPÉENNE 2002/58 COMME AMORCE D'UNE TROISIÈME GÉNÉRATION

39. La deuxième génération qui englobe la directive dite générale de protection des données de même que l'article 8 de la Charte européenne des droits de l'homme qui en est le prolongement semble aujourd'hui insuffisante à prendre en compte les risques encourus par les libertés des citoyens du fait des technologies de l'information et de la communication. On rappellera que la directive de 1995 n'a pu prendre en compte le fait de l'Internet et des nouveaux réseaux numériques, ni d'ailleurs la directive 97/66/CE dite RNIS et vie privée.

La prise en considération de ces nouveaux réseaux et des utilisations dont on perçoit seulement aujourd'hui les premiers développements amène à devoir considérer un élargissement de la protection des données au-delà des principes mis en place par la directive 95/46/CE.

Si la technologie de l'information et de la communication est prise en compte en 1995, son impact est perçu du seul côté du responsable comme

[103] "16. *Les trois institutions rappellent que la Communauté (européenne) ne légifère que dans la mesure nécessaire, conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité. Elles reconnaissent l'utilité de recourir, dans les cas appropriés, ..., à des mécanismes de régulation alternatifs*" (Point 16 de l'accord institutionnel cité note 80).

un accroissement de leurs pouvoirs et crée dès lors des obligations à la charge de ces derniers de veiller à la sécurité technique et organisationnelle des traitements, la notion de sécurité étant entendue au sens le plus large.

40. La révolution que représentent les réseaux numériques pour la protection des données repose sur le fait qu'entre le responsable du traitement tel que conçu par la directive et la personne concernée, la technologie s'interpose à un double titre. Comme nous l'avons montré, elle est à la base de flux conscients ou inconscients provenant du terminal de la personne concernée ou d'un objet qui autorise le contact avec cette personne, même non identifiée voire non identifiable. Par ailleurs, le réseau lui-même ne constitue plus, comme c'était le cas dans la communication par circuits, un lien unique entre un émetteur et un destinataire mais autorise un foisonnement de relations non contrôlées où interviennent, à partir de lieux multiples et sans considération de frontières, des intervenants connus ou inconnus.

Bref, c'est cette technologie d'interface entre la personne concernée et ces intervenants qu'il importe désormais de réglementer. A notre opinion, la directive 2002/58/CE contient les éléments de base de cette nouvelle approche.

41. Traditionnellement, la directive de 2002 est considérée comme une application ou spécification[104] des règles contenues dans la directive de 1995 dite directive générale. Elle constitue une révision de la directive sectorielle 97/66/CE du 15 décembre 1997 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[105] et l'adaptation de cette dernière à l'évolution du marché des technologies et des services de communication et aux risques nouveaux liés à cette évolution.

Notre propos est de suggérer une autre lecture : l'adoption de la directive de 2002 marque sur certains points limités certes mais importants une

[104] A cet égard, lire S. LOUVEAUX et M. V. PEREZ-ASINARI, "*New European Directive 2002/58 on the processing of personal data and the Protection of Privacy in the Electronic Communications Sector*", (2003) CTLR, 5, p. 133 ; W. MAXWELL (ed.), *Electronic Communications : The new EU Framework : Booklet I.5 : The Communications Data Protection Directive,* Oceana, Dobbs Ferry, New York, 2002.

[105] Directive 97/66/CE relative aux traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *J.O.* 24 janvier 1998, p. 1.

rupture avec la conception traditionnelle de la protection de la vie privée, consacrée par la directive 95/46/CE[106]. Notre thèse s'appuie sur le fait qu'à la fois en ce qui concerne les données protégées, les personnes soumises à des obligations et les objets réglementés, la directive de 2002 déborde le champ d'application de celle de 1995.

42. La définition même des "données", dont la protection est au cœur même de la directive récente ne suit pas exactement celle de 1995. Les définitions de "données de trafic" et de "localisation" reprises à l'article 2 évitent soigneusement les expressions de "données à caractère personnel", qui circonscrivent pourtant le champ d'application de la directive 95/46/CE, dont la directive de 2002 ne serait qu'une application. Autant, l'article 2 c) que le considérant 14 de la Directive définit la donnée de localisation par la seule référence à l'équipement terminal d'un utilisateur. Lorsqu'il s'agit de commenter la notion de donnée de trafic, le considérant 15 parle "d'informations consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication".

Qu'est-ce à dire ? Ces données peuvent ne pas être des données à caractère personnel, en d'autres termes que la recherche du lien avec une personne identifiée ou identifiable n'est plus nécessaire. Sans doute, dira-t-on, l'article 3 à propos des "services concernés" par la directive n'évoque que les "traitements de données à caractère personnel dans le cadre de la fourniture de services de communications dans la Communauté". Dans la mesure où d'autres dispositions de la directive, comme il sera montré plus loin, réglementent des situations qui excèdent le champ d'application de l'article 3, on n'y prêtera pas nécessairement attention. Il suffit en effet selon la définition de la donnée de trafic ou de localisation qu'un lien puisse être fait avec un terminal, un objet et qu'à travers celui-ci une personne, le possesseur de ce terminal même non identifié puisse soit être atteint, soit être caractérisé pour que cette directive nouvelle s'applique. Une telle conception permettrait demain de réglementer les systèmes d'intelligence ambiante, fondés sur des techniques de RFID qui entendent manipuler des données relatives à un objet pour prendre des décisions vis-à-vis de leurs possesseurs sans s'intéresser à "identifier", au sens classique du terme, ces derniers. En d'autres termes c'est la possibilité, grâce à des données, de prendre des décisions vis-à-vis de certains individus identifiés ou non, identifiables ou non, qui doit être entourée de garanties.

[106] A ce propos, l'article 1.2. de la directive 2002/58 note à juste titre : "Les dispositions de la présente directive précisent et complètent la directive 95/46/CE ...".

Prenons, par exemple, un service d'aide à la "navigation touristique" lancé par une commune et fondé sur un réseau d'intelligence ambiante et une technologie RFID. En tant qu'utilisateur de ce système, non obligé de m'identifier, je génère au cours de ma promenade des données de localisation qui me permettent de me repérer et, le cas échéant, d'avoir des informations sur les richesses artistiques que je croise. Voilà certes des données de localisation relatives aux utilisateurs visées par l'article 9 de la directive 2002/58/CE. S'agit-il de données à caractère personnel ? Par hypothèse, selon la directive de 1995, non ... du moins si aucun lien avec l'identité du porteur du terminal ne peut être fait. On imagine cependant parfaitement l'application de certains articles de la directive 2002/58/CE à de telles données sans caractère personnel : ainsi, l'article 9 en matière d'obligation d'informations du fournisseur de services et en matière de restriction de la durée d'utilisation de ces services et des personnes ayant accès aux données générées. Le même article ne légitimerait le traitement de données que sur base du consentement, celui-ci pouvant être retiré à tout moment (un simple bouton désactivant l'émission d'ondes radio).

Bref, la directive 2002/58/CE apparaît applicable en dehors des seules données dites à caractère personnel.

43. A propos des personnes assujetties à la directive 2002/58/CE, on peut comprendre de la même manière la volonté des auteurs de la directive d'éviter soigneusement à propos du fournisseur de services de communication, la notion de "responsables du traitement" au sens de la directive générale. On peut en effet imaginer que le fournisseur d'un service de communication enregistre des données relatives à l'utilisation de terminaux pour lesquels le lien avec l'identité de l'utilisateur soit pratiquement impossible. Ainsi, l'activité de tout fournisseur de service de communication, c'est-à-dire dont l'activité consiste en l'acheminement des données ou des réseaux ou en l'accès à de tels réseaux est réglementée sans nécessairement se fonder sur les règles de la directive générale. Ainsi, les hypothèses de légitimité d'un traitement des données acheminées sont très limitées. Cette restriction s'explique par la nature même de leur intervention, qui est dictée par la seule technologie de communication qui s'impose à tout qui utilise des réseaux.

Cette situation particulière d'interface explique le rôle que ces fournisseurs peuvent jouer comme "collaborateur" de l'autorité publique dans la recherche d'informations relatives à l'utilisation des réseaux qui pour-

raient conduire à l'identification de délinquants[107]. Ce rôle justifie, on le pressent, la mise sur pied de système de cahiers des charges ou d'agrément applicables à ces acteurs d'une nature particulière.

44. D'autres dispositions de la directive témoignent bien plus encore de cette approche nouvelle. L'article 5.3 traite de l'utilisation des réseaux de communication en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur. L'article 14 évoque lui les caractéristiques techniques et la normalisation des équipements terminaux pour préciser au point 3 que, nonobstant le principe du libre marché, des normes peuvent être imposées à la construction de ces équipements afin de les rendre comparatifs avec le droit des utilisateurs de protéger et contrôler l'utilisation de leurs données à caractère personnel.

Le rapprochement de ces deux dispositions se justifie par le fait qu'elles concernent toutes deux les équipements terminaux et qu'elles constituent des dispositions clairement en dehors du domaine d'application de la directive, domaine fixé comme il a été rappelé par l'article 3.1. de la directive commentée. Elles ne concernent en effet pas des traitements de données opérées dans le cadre de la fourniture de services de communications électroniques.

Leur présence est donc d'autant plus significative.

45. La première disposition entend prévenir toute intrusion dans l'équipement terminal. On songe aux cookies, aux spywares mais également à des applications plus légitimes permettant par exemple la mise à jour à distance de programmes téléchargés sur l'ordinateur. L'article vise à donner à l'intéressé une maîtrise plus complète de son équipement, en obligeant le responsable de cette intrusion (le responsable du traitement des données)[108] à donner certaines informations à l'utilisateur du terminal sur la finalité de l'intrusion et à lui permettre de refuser cette dernière.

[107] C'est tout le débat sur le fameux article 15 de la directive à propos du droit des États de demander la conservation des données de trafic. Le débat a abouti à la directive 2006/24/CE du 16 mars 2006 relative à la rétention des données de trafic traitées en relation avec la délivrance de services de communications électroniques et amendant la directive 2002/58, directive adoptée en mars 2006.

[108] La mention de données à caractère personnel n'est pas utilisée. On note ici aussi que la question est abordée sans qu'on s'interroge sur l'existence ou non d'un traitement de données à caractère personnel. C'est l'équipement terminal qui en tant que tel est visé et qui fait l'objet de la protection réglementaire. On sait que la question de savoir si les cookies sont des données à caractère personnel est loin d'être tranchée. Cette disposition rend ce débat inutile.

AIDC, VOLUME XVII, Droit constitutionnel et vie privée, Tunis 2007

L'article 14[109] de la directive 2002/58/CE prolonge cette première disposition relative au terminal. Dans la mesure où ce sont les spécifications techniques de fonctionnement du terminal qui permettent ces intrusions ou de manière plus générale certaines atteintes à la protection des données, la Commission se réserve le droit d'imposer aux fabricants d'équipements certaines normes qui assurent la compatibilité du terminal avec le respect des exigences de protection des données.

46. Notre propos était de montrer l'attention que la directive 2002/58/CE donne, au-delà des questions traditionnelles de protection des données à caractère personnel, au fait technologique que représente le fonctionnement des réseaux, et ce indépendamment des rapports entre la personne concernée et les responsables de traitement, chacun situé aux extrémités du réseau.

Ainsi, la directive permet l'extension de la protection à des catégories de données qui ne sont point nécessairement qualifiables de données à caractère personnel dans la mesure où elles sont liées à des terminaux et non à des personnes.

Ainsi, la directive 2002/58/CE dite "vie privée et communications électroniques" pointe le rôle particulier de deux acteurs, indépendamment de leur qualité de responsables de traitement :

- les opérateurs de réseaux (en ce compris les fournisseurs d'accès à Internet), c'est-à-dire ceux qui fournissent "des systèmes de transmission et le cas échéant, les équipements de communication ou de routage et les autres ressources qui permettent l'acheminement de signaux"[110] qui constituent des interfaces obligés entre l'utilisateur du réseau en tant que personne concernée et les multiples acteurs de l'Internet qui pourront traiter les données multiples générées consciemment ou non par l'utilisation du réseau. C'est à eux qu'incombent certains devoirs, tels celui de prévenir des risques liés à l'utilisation du réseau, de garantir la sécurité de ses

[109] Cet article se fonde sur la disposition de la directive 1999/5/CE (du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *JOCE* n° L 091 du 7 avril 1999 pp. 10-28) qui, parmi les "essential requirements" qui doivent être respectés par les producteurs ou distributeurs d'équipements terminaux, prévoit outre les questions de sécurité des utilisateurs ou des prestataires du réseau, la protection de la vie privée des utilisateurs.

[110] Directive 2002/21/CE, article 1(d).

services, de permettre des restrictions à l'identification de la ligne appelante, etc. ;

- les fournisseurs d'équipements terminaux, en particulier -mais non uniquement-, des logiciels de navigation, dont les caractéristiques techniques doivent mettre en œuvre les dispositions de la directive. En particulier, la directive prévoit la possibilité d'imposer certaines "mesures afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel".

47. Cette extension doit se concevoir comme un complément des deux premières approches. Comme il a été montré, la deuxième approche signifiait déjà une rupture avec la première dans la mesure où la notion de vie privée, préoccupation à l'origine des lois de protection des données, s'est effacée au profit d'un régime général de protection des données à caractère personnel et par l'octroi de droits subjectifs aux personnes concernées et d'obligations précises pour les responsables de traitement. La troisième approche ne remet pas en cause ces deux premières approches. Au contraire, elle s'y enracine mais la prise en compte des risques nouveaux liés aux réseaux de communication électronique conduit à un nouvel élargissement de la protection des libertés des citoyens.

II. OÙ IL EST QUESTION DE NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES PERMETTANT D'ASSURER AUX PERSONNES UNE PROTECTION ADÉQUATE DANS L'ENVIRONNEMENT DES RÉSEAUX MODERNES DE COMMUNICATIONS ÉLECTRONIQUES

48. Les caractéristiques de l'environnement des services de communication électronique (omniprésence, complexité, opacité, performance et polyvalence) et des terminaux (interactivité, dimension internationale, opacité de fonctionnement) créent de nouveaux risques et aggravent les risques d'atteinte aux libertés individuelles et à la dignité humaine.

La parade à ces risques n'est possible que par la consécration de principes nouveaux améliorant la protection des individus et lui donnant une meilleure maîtrise de leur environnement. Ce n'est en effet que dans la mesure où cette maîtrise est possible que la personne concernée pourra prendre effectivement la responsabilité de sa propre protection et mieux disposer des moyens d'une véritable autodétermination informationnelle.

La formulation de ces nouveaux principes est une première tentative de ce qui pourrait, au-delà des prescrits de la directive 2002/58/CE que nous

venons d'analyser, constituer les bases d'une troisième génération de législation de protection des données.

A. Premier principe : Du chiffrement et de l'anonymat "réversible"

49. Le chiffrement des messages assure la protection de l'accès au contenu des communications. Leur qualité varie et les techniques de chiffrement et de déchiffrement peuvent également être diverses. Les logiciels d'encryptage placés sur l'ordinateur de l'internaute (par exemple, SSL ou PGP) sont désormais accessibles à des prix abordables et généralement intégrés dans les logiciels grand public. La notion d'anonymat devrait sans doute être redéfinie et, dans la foulée, d'autres termes comme "pseudonyme" ou "non identifiabilité" devraient être préférés dans la mesure où cette notion d'anonymat demeure ambiguë. Ce qui est recherché est bien souvent, non un anonymat absolu, mais une "non identifiabilité" fonctionnelle de l'auteur d'un message vis-à-vis de certaines personnes[111]. Nombre de textes à caractère non contraignant préconisent le "droit" du citoyen[112] à disposer de l'anonymat lorsqu'il utilise les services offerts par les technologies nouvelles. La Recommandation n° R(99) 5 du Comité des Ministres du Conseil de l'Europe[113] énonce, nous le rappelons, le même principe : "L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée" et souligne à ce propos l'intérêt des "Privacy Enhancing Technologies" disponibles sur le marché. Au-delà, on connaît les prescrits de la directive

[111] Sur ce point, lire J. GRIJPINK et C. PRINS, "*Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions ?*", 17 *CL&SR* (2001), pp. 378 et ss.

[112] A ce propos, lire notamment S. RODOTA, "Beyond the E.U. Directive : Directions for the Future", *in Privacy : New Risks and opportunities*, Y. POULLET, C. DE TERWANGNE et P. TURNER (ed.), *Cahier du CRID*, n° 13, p. 211 et ss.

[113] Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "inforoutes", texte disponible sur le site du Conseil de l'Europe. Dans le même sens, la recommandation 3/97 du groupe dit de l'article 29 intitulée : "l'anonymat sur Internet". *Cf.* également l'avis de la Commission belge de la vie privée pris d'initiative sur le commerce électronique (Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission belge de la vie privée : *http://www.privacy.fgov.be*) rappelle à bon escient qu'il existe des mécanismes qui permettent d'authentifier l'émetteur d'un message sans nécessairement l'obliger à s'identifier.

A.I.D.C., Volume XVII, Droit constitutionnel et vie privée, Tunis 2008

2002/58/CE qui permettent à l'utilisateur d'un terminal téléphonique[114] d'éviter la présentation de la ligne appelante et de la ligne connectée. L'article 9.2. de la même directive rend obligatoire la possibilité, pour l'utilisateur d'un terminal permettant la géo-localisation et qui ne s'est point opposé au départ à cette possibilité, d'interdire temporairement le traitement de ces données pour chaque connexion ou pour chaque transmission de communication.

50. En d'autres termes, celui qui utilise les moyens modernes de communication devrait avoir le choix de rester non identifiable au regard, tantôt de tiers intervenant dans l'acheminement du message ou de prestataires intervenant dans cette chaîne de communication, tantôt du ou des destinataires de la communication et disposer gratuitement, ou au moins à des prix abordables, des moyens d'exercer son choix[115]. La mise à disposition à des coûts abordables de moyens ou de services de chiffrement et d'anonymisation est une condition nécessaire à une responsabilisation de l'internaute.

L'anonymat ou la "non identifiabilité fonctionnelle" requis ne sont cependant pas absolus. Au droit à l'anonymat des citoyens, s'oppose l'intérêt supérieur de l'État qui pourra imposer des limitations lorsque celles-ci constituent des mesures nécessaires "pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite de (certaines) infractions pénales". L'équilibre entre le légitime contrôle des infractions et la protection des données pourrait être trouvé dans des systèmes de "pseudo-identité" attribuée à un individu par un fournisseur de service spécialisé auprès duquel, dans les seuls cas prévus par la loi et moyennant les modalités fixées par celle-ci, pourrait s'opérer le lien entre l'identité réelle d'un usage et son pseudonyme.

[114] *Cf.* l'article 8.1 de la directive qui précise que cette présentation doit pouvoir être évitée par un moyen simple et gratuit. Un tel prescrit a des conséquences sur la configuration de l'appareil terminal.

[115] *Cf.* à cet égard, la recommandation de la CNIL suivant laquelle tout accès à un site marchand doit être possible sans que l'internaute n'ait à s'identifier préalablement (M. GEORGES, "Relevons les défis de la protection des données à caractère personnel : l'Internet et la CNIL", *in Commerce électronique, marketing et vie privée*, Ph. LEMOINE (éd.), Paris, LaSer, 1999, pp. 71 et 72. *Cf.* également, le document de travail du groupe dit de l'article 29 à propos des systèmes d'authentification en ligne et en particulier de Netpassport (W.P. 68, 29 Janvier 2003).

AIDC, VOLUME XVII, Droit constitutionnel et vie privée, Tunis 2007

Au-delà, d'autres solutions pourraient être imposées par une réglementation des appareils terminaux : suppression du "bavardage" des navigateurs, la création d'adresses éphémères ou relatives à un groupe d'individus et une différenciation des données d'adressage suivant les tiers qui auront accès aux données de trafic ou de localisation et la disparition des pointeurs (Global Unique Identifiers) par l'uniformisation des protocoles d'adressage.

51. Nos réflexions sur les terminaux identifiant des objets à défaut des personnes qui les possèdent amènent à élargir le propos. Ne peut-on considérer que c'est un droit pour l'utilisateur d'un tel terminal de supprimer le fonctionnement de ce terminal : ainsi la personne promenant son caddie dans une grande surface fonctionnant comme un système d'intelligence ambiante, a le droit de désactiver à tout moment le RFID qui permet de contrôler ses mouvements voire de les guider[116].

Dernière remarque : le statut des "anonymisers", véritable tiers de confiance pour celui qui y fait appel, devrait être réglementé afin d'offrir, d'une part, à celui qui y recourt certaines garanties quant à la qualité des services offerts et, d'autre part, à l'État, la garantie de pouvoir techniquement accéder au contenu des télécommunications, dans les conditions prévues par la loi[117].

B. Deuxième principe : La réciprocité des avantages

52. Ce principe pourrait s'exprimer comme suit : le législateur met à charge de celui qui utilise la technologie aux fins de développer ses activités professionnelles, certaines obligations supplémentaires qui permettent de rétablir l'équilibre traditionnel des parties en présence. La justification du principe est simple. Si la technologie accroît les capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d'opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concer-

[116] En ce sens, la Résolution de la 25ème conférence internationale de Commissaires à la protection des données, prise à Sydney en 2003 (*http://www.privacy.conference2003.org*) : "chacun ... devrait avoir la possibilité de supprimer, désactiver ou détruire les étiquettes".

[117] La qualité des services offerts et des exigences de confidentialité pourrait faire l'objet d'un cahier des charges, comme il en est proposé en matière de signatures électroniques. L'agréation d'un "anonymiser" reconnaîtrait son respect du cahier des charges. On peut concevoir que l'agréation ne soit pas requise mais volontaire, équivalent dans ce cas à un label de qualité.

née, l'administré, le consommateur, bref le fiché, puisse bénéficier, dans une proportion comparable, des avantages de cette technologie.

Quelques dispositions récentes se fondent sur l'exigence de la réciprocité des avantages pour obliger celui qui utilise des technologies à mettre à disposition de l'internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits qui peuvent être mis à mal par l'utilisation de ces moyens électroniques.

53. Les exemples législatifs tirés des directives européennes récentes ne manquent pas. Ainsi, premier exemple, la directive européenne 2001/31/CE sur les services de la société de l'information prévoit la possibilité de s'opposer *via des moyens électroniques* au spamming. En d'autres termes, celui qui utilise, pour diffuser de manière plus efficace et rapide ses messages publicitaires, les technologies de l'information et de la communication doit accepter que le destinataire utilise les mêmes voies pour s'opposer à toute diffusion ultérieure. Deuxième exemple déjà cité : l'article 5.3 de la directive 2002/58/CE "Vie privée et communications électroniques" exige de même que toute "utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou utilisateur doit faire l'objet d'une information de ce dernier et que celui-ci dispose du droit de refuser un tel traitement ...". Les commentateurs insistent sur le fait qu'un tel refus doit pouvoir s'exprimer par un moyen aisé, un simple clic à partir du terminal et non l'utilisation d'une correspondance écrite. Enfin, troisième exemple : la possibilité pour l'abonné (article 8.1 de la directive 2002/58/CE) de restreindre "par un moyen simple et gratuit l'identification de la ligne appelante et ce, appel par appel ... et ce, pour chaque ligne" est une autre manifestation, riche d'applications possibles si l'on veut bien suivre le raisonnement proposé dans le premier principe. Cette possibilité de restriction d'identification de la ligne appelante conduit à une obligation corrélative pour le fournisseur du service de permettre, par un moyen simple et gratuit, poursuit la directive, au destinataire soit de refuser les appels entrant non identifiés, soit d'empêcher leur identification (article 8.2 et 8.3).

54. Au-delà, dans le cadre des réseaux de communication électronique, on peut de même envisager que certains droits de la personne concernée, ainsi le droit à l'information, le droit d'accès et de rectification et le droit de recours puissent demain se réaliser par des moyens électroniques que permet le fonctionnement interactif du réseau. De multiples applications de ce droit peuvent dès maintenant être suggérées.

AIDC, VOLUME XVII, *Droit constitutionnel et vie privée*, Tunis 2007

Le droit à l'information de la personne concernée doit pouvoir s'opérer à tout moment par un simple clic (ou plus largement par un simple geste positif, électronique et immédiat) sur un sigle permettant l'accès à une "Privacy Policy" dont on peut espérer qu'elle soit d'autant plus précise et complète que le coût de la diffusion est réduit dans le cas de l'utilisation du média électronique. Cette démarche doit rester anonyme pour le serveur de la page (crainte de "fichage" des internautes "privacy concerned or minded"). Au-delà, en cas de labellisation du site, on peut songer à rendre obligatoire l'existence d'un hyperlien qui permettrait à partir du sigle du label de visiter la page du site de l'organe de labellisation relative au site web en question. Même suggestion à propos de la déclaration d'un maître du fichier à l'autorité de contrôle, un hyperlien serait ainsi placé sur une page incontournable du site web, objet du traitement déclaré et la page du site de l'autorité de contrôle reprenant la déclaration du site concerné.

Le droit d'accès de la personne concernée doit demain pouvoir s'exercer via le média électronique sur base de l'utilisation de la signature électronique. Il devrait obliger la personne responsable à structurer ses fichiers de manière à permettre à la personne d'exercer de façon aisée ce droit d'accès. Des renseignements complémentaires comme l'origine des données, la liste des tiers à qui communication de certaines données a été faite devraient être systématiques.

Au-delà, notons que dans les vastes réseaux publics et privés, la donnée à caractère personnel n'est plus collectée pour une ou des finalités précises mais "déposée" à un endroit du réseau pour servir à des finalités définies de manière évolutive en fonction des capacités de traitement nouvelles ou de besoins non aperçus au départ. Face à cette réalité, il importe que la personne concernée puisse obtenir une documentation décrivant les flux au sein du réseau, les données en question et les divers utilisateurs, bref ce qu'on peut appeler un "cadastre des flux"[118].

Les droits de rectification et/ou d'opposition devraient pouvoir faire l'objet de réclamations en ligne auprès d'une personne désignée chargée de l'examen de plaintes ou de gérer la liste des oppositions, acteur dont le statut devrait être défini.

[118] Cette idée a été reprise par deux lois belges récentes qui créent des comités sectoriels en lien avec le registre national (Loi du 8 août 1983 organisant un registre national des personnes physiques modifiée par la loi du 25 mars 2003, M.B. 28 mars 2003, art.12 § 1) et le second en lien avec la Banque Carrefour des entreprises (Loi du 16 janvier 2003 portant création d'une Banque Carrefour des entreprises, M.B. 5 février 2003, article 19 § 4).

A.I.D.C., Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2008

Le droit de recours, également, ne mériterait-il pas de pouvoir bénéficier des avantages que représente la cybermagistrature : saisine on-line, gestion de l'échange par voie électronique des arguments des deux parties et finalement prononcé de la décision ou de la proposition de médiation ?

Le droit lorsqu'une décision soit automatisée, soit signifiée par le biais d'un réseau est opposée à la personne concernée (ainsi, refus d'un permis de bâtir suite à une procédure dite de télé-administration), devrait pouvoir connaître par le même canal la logique suivie pour la prise de décision. A cet égard, en matière de service public[119], le citoyen devrait pouvoir bénéficier du droit de pouvoir tester de manière anonyme les logiciels d'aide à la décision ou systèmes expert qui pourront lui être appliqués le cas échéant (ainsi, un logiciel d'aide au calcul automatique des impôts ou des primes susceptibles d'être obtenues en matière de réhabilitation d'un logement).

C. Troisième principe : La promotion de solutions technologiques conformes au respect des principes de protection des données ou améliorant la situation des personnes protégées par le droit

55. La Recommandation 1/99 du 23 février 1999[120], émise par le groupe dit de l'article 29 sur base d'une analyse des risques créés pour la vie privée par les logiciels et matériels utilisés pour la communication via Internet, émet le principe suivant lequel l'industrie du logiciel et du matériel se devait de développer des produits en conformité avec les dispositions des directives en matière de protection des données personnelles. Ce troisième principe, répété dans d'autres avis du groupe dit de l'article 29[121], conduit à reconnaître aux régulateurs diverses modalités d'intervention.

Ainsi, il s'agit pour lui de pouvoir intervenir en cas de développements technologiques présentant des risques majeurs. Ce principe dit de "pré-

[119] Pour les décideurs privés, le principe est le même sous réserve des intérêts légitimes du maître du fichier (en particulier, le secret des affaires qui pourrait atténuer le devoir d'expliciter la logique suivie).

[120] Recommandation sur les traitements invisibles et automatiques de données à caractère personnel sur Internet réalisés par des logiciels et matériels utilisés pour la communication via Internet.

[121] Ainsi, dans le document relatif aux RFID : *Working Document on Data Protection issues related to RFID technology*, 19 janvier 2005 déjà cité.

A.I.D.C., Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2007

caution" largement connu en droit de l'environnement[122] pourrait trouver à s'appliquer en matière de protection des données. Au nom de ce principe de précaution, il apparaît d'ailleurs comme nécessaire que les équipements terminaux de télécommunication (en ce compris les logiciels qui les animent) adoptent le paramétrage par défaut le plus protecteur possible, de manière à ce que la personne concernée ne puisse pas, par défaut, être exposée à divers risques qu'elle ignore ou qu'elle ne sait mesurer.

56. Par ailleurs, au nom du principe de réciprocité des avantages, il paraît opportun et non déraisonnable de doter certains équipements terminaux de télécommunications, de "journaux de bord", à l'instar de ce qui se fait pour les logiciels de type "serveur" déployés par les entreprises et les administrations en ligne. Ceci permettrait à chaque utilisateur d'apprécier et de contrôler les personnes qui ont eu accès à son équipement et, le cas échéant, de visualiser les caractéristiques essentielles des transferts d'informations entrant et sortant.

Une disposition de la directive européenne "vie privée et communications électroniques" déjà citée, pourrait servir de base à cette obligation mise à charge des fabricants de terminaux. L'article 14 prévoit qu'en cas de non-conformité d'un équipement terminal aux règles de protection des données, la Commission peut prendre des initiatives en matière de standardisation de ceux-ci. En d'autres termes, la normalisation technique des équipements terminaux constitue une mesure -certes subsidiaire- d'assurer la protection des données à caractère personnel contre les risques de certains traitements abusifs, risques créés par les choix technologiques.

57. Au-delà, au nom du principe de sécurité, prescrit par l'article 7 de la Convention n° 108 du Conseil de l'Europe, il s'agit d'interdire les "Privacy Killing Technologies"[123]. L'obligation de prévoir des mesures tech-

[122] Sans doute, serait-il utile de développer la comparaison entre les modes de régulation de ces deux problématiques : la privacy, d'une part et l'environnement, d'autre part vu les similarités des contextes : caractère transnational des enjeux, dimension technologique importante et la similarité des approches : auto ou co-régulation du secteur, droit à l'information des personnes concernées, principe de sécurité, ...

[123] Selon l'expression de J.-M. DINANT, "Law and Technology Convergence in the Data Protection Field ? Electronic threats on personal data and electronic data protection on the Internet", *in E-commerce law and practice in Europe*, Ed Ian WALDEN & Julia HORNLE, under the auspices of the Eclip Network, Wood Head Publishing Limited, Cambridge, Avril 2001.

niques et organisationnelles appropriées aux risques engendrés pour la protection des données conduira le responsable d'un site à veiller à la confidentialité des messages échangés, à signaler clairement les transmissions de données -fussent-elles automatiques et par hyperlien comme c'est le cas avec les sociétés de cybermarketing- et à lui donner les moyens aisés de les bloquer.

Cette même obligation de sécurité a pour conséquence d'imposer à celui qui développe des terminaux, le choix de solutions technologiques aptes à minimiser voire à réduire à néant les risques d'atteinte à la vie privée. L'influence de ce prescrit sur le design des cartes à puce, en particulier les cartes multifonctionnelles[124] comme les cartes d'identité, est évident.

58. Peut-on aller plus loin et recommander le développement de "Privacy Enhancing Technologies", c'est-à-dire d'outils ou de systèmes qui permettent de mieux assurer le respect des droits de la personne concernée[125] ? Il est certain que c'est le marché qui, librement, développera ces technologies mais la promotion de telles solutions "privacy compliant" ou "privacy enhancing" exige plusieurs rôles actifs de l'État : celui de veiller par des subsides à la recherche et au développement de ces solutions ; celui de mise en place de systèmes volontaires de certification ou d'accréditation des solutions élaborées et d'assurer la publicité de ces "labels" ; celui de mettre à disposition à des coûts "abordables" les solutions technologiques considérées comme nécessaires à la protection des

[124] Voir à ce sujet, J.-M. DINANT and E. KEULEERS, *Part 1 :* "Data protection : multi-application smart cards. The use of global unique identifiers for cross-profiling purposes". *Part 2 :* "Towards a privacy enhancing smart card engineering", *in CL & SR*, Vol. 20, n°1, 2004, pp. 22-28, Elsevier, Oxford, 2004.

[125] On souligne que cette volonté de développer les PETS (Privacy Enhancing Technologies) est un des axes majeurs de la politique du groupe dit de l'article 29 et de la Commission. Un séminaire s'est tenu à cet égard le 4 juillet 2003. On note dans le Rapport de la Commission sur la mise en œuvre de la directive 95/46/CE établi par la Commission et publié le 15 mai 2003 (COM(2003) 205 final, rapport disponible sur le site de la Commission) que le point 8 des initiatives européennes pour une meilleure application de cette directive est précisément la promotion des technologies renforçant la protection de la vie privée : "La Commission, note le rapport, travaille déjà, dans le domaine des technologies renforçant la protection de la vie privée, notamment au niveau de la recherche comme par exemple, les projets RAPID et PISA ... Elle invite les autorités nationales de contrôle à poursuivre les discussions sur la question des technologies permettant de renforcer la protection de la vie privée et de réfléchir sur les mesures que les autorités nationales de contrôle pourraient prendre ...".

A.I.D.C., Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2008

A.I.D.C., Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2007

données[126] ; celui, enfin, de réprimer de manière sévère, le contournement de telles mesures de protection, comme il l'a fait à propos des mesures de protection de la propriété intellectuelle[127].

D. Quatrième principe : La maîtrise par l'utilisateur du fonctionnement des équipements terminaux

59. La justification du principe est évidente. Dans la mesure où ces terminaux permettent à autrui de capter nos comportements, nos actions ou simplement de nous localiser, leur fonctionnement doit être transparent et sous notre contrôle. L'article 5.3 de la directive 2002/58/CE déjà citée en est une première illustration. La personne doit être clairement informée de toute utilisation à distance de son terminal (cookies, spyware) et pouvoir facilement et gratuitement s'y opposer. La règle posée par la directive 2002/58/CE qui permet à l'utilisateur d'une ligne appelante ou connectée de pouvoir empêcher la présentation de l'identification de la ligne appelante ou appelée constitue une autre illustration du principe.

Au-delà de ces exemples, on pose le principe que tout équipement terminal devrait être paramétré de telle manière que son possesseur ou utilisateur puisse être informé de manière complète des flux entrants et sortants et puisse agir en connaissance de cause, s'il l'estime nécessaire.

De même, la possession d'une carte à puce devrait être accompagnée, comme le prévoient certaines législations sur les cartes d'identité électronique, d'une possibilité d'accès en lecture des données inscrites sur la carte, par la personne concernée. La maîtrise suppose également, nous l'avons dit, que la personne puisse à tout moment décider de désactiver définitivement le terminal. En matière de RFID, la question est importante. La personne concernée doit pouvoir, gratuitement et facilement,

[126] Sur ce point, nos réflexions in "Comment "réguler" la protection des données ? Réflexions sur l'internormativité ?", *Mélanges P. DELNOY*, Larcier, 2005, à paraître. A cet égard, relevons que les technologies qualifiées de PET peuvent s'avérer "privaticides", lire sur ce point le débat à propos du P3P, entre ROTENBERG et LESSIG in "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get ?)", 2001 *Stanford Technology Law Review*, 1.

[127] *Cf.* l'article 6 de la directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects de la propriété intellectuelle et des droits voisins dans la société de l'information.

A.I.D.C., Volume XVII, Droit constitutionnel et vie privée, Tunis 2008

auprès de tiers fiables[128] s'assurer de la désactivation de ce moyen technique de repérage à distance.

On note que l'usager devra pouvoir opposer ce principe à des entreprises non nécessairement visées par les réglementations classiques de protection des données dans la mesure où elles ne sont point responsables de traitement : ainsi les fournisseurs d'équipements terminaux et des multiples logiciels en particulier de navigation susceptibles d'être incorporés au terminal pour faciliter la réception, le traitement ou l'émission de communications électroniques.

Au-delà, il s'adresse aux organes de normalisation tant publics que privés qui s'occupent ou se préoccupent de la configuration de ces équipements.

60. L'idée essentielle est que les produits mis à la disposition des usagers des services de communications électroniques ne puissent permettre de par leur configuration même des agissements illicites, qu'ils soient le fait de tiers ou du producteur lui-même. Quelques exemples illustrent l'importance du propos :

- la comparaison des navigateurs présents sur le marché démontre que le bavardage de certains d'entre eux va bien au-delà de ce qui est strictement nécessaire à l'établissement de la communication[129] ;

- le traitement de la réception, de la suppression et du blocage d'envoi des cookies diffère d'un navigateur à l'autre. Ainsi, suivant les programmes de navigation et leur configuration, des traitements déloyaux seront plus ou moins faciles ; le blocage des fenêtres "pop-up" ou de l'envoi systématique des références des articles lus en ligne ou des mots-clés frappés sur les moteurs de recherche ne semble tout simplement pas possible ou, en tous cas, pas possible de manière simple sur le navigateur installé par défaut sur la plupart des centaines de millions d'ordinateurs personnels ;

- l'utilisation d'identifiants globaux uniques (GUID) ou de logiciels espions est également à signaler.

61. Par ailleurs, on s'interroge sur la nécessité d'équipements terminaux transparents dans leur fonctionnement permettant à leur usager d'avoir la pleine maîtrise des données envoyées et reçues. Ainsi, l'usager devrait pouvoir connaître de manière conviviale l'étendue exacte du bavardage

[128] On songe bien évidemment à des systèmes de labellisation ou à des agréments donnés par l'autorité publique à certaines entreprises.

[129] A ce sujet, J-M DINANT, "Le visiteur visité, Quand les éditeurs de logiciel Internet passent subrepticement à travers les mailles du filet juridique", *in Lex Electronica*, vol. 6, n° 2, hiver 2001.

AIDC, VOLUME XVII, Droit constitutionnel et vie privée, Tunis 2007

de son ordinateur, les informations transmises et reçues, leur finalité et leur émetteur ou leur destinataire. A cette fin le journal de bord apparaît comme une technique appropriée et relativement aisée à mettre en œuvre.

Au-delà de ce droit de l'utilisateur d'être informé des flux entrants, on peut s'interroger sur le droit de la personne de soumettre à autorisation le fait pour un tiers de pénétrer son "domicile virtuel". Il convient ici de rappeler les dispositions de la Convention du Conseil de l'Europe concernant la Cybercriminalité et notamment ses articles 2[130] (accès illégal) et 3[131] (Interception illégale).

On remarquera ici que l'identification ou l'identifiabilité des personnes participant à une télécommunication ne constitue pas une condition d'application de cette Convention. Semblablement, l'accès non autorisé à un système informatique ne se limite pas au hacking de gros systèmes informatiques appartenant à des banques ou à des administrations mais concerne aussi l'accès non autorisé à un terminal de télécommunication qui, en l'état actuel de l'art, est un ordinateur[132] et ce indépendamment de toute infraction aux lois protégeant les données à caractère personnel. L'intrusion dans un terminal est en soi une infraction[133], une forme de "hacking".

[130] Article 2. Accès illégal : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

[131] Article 3. Interception illégale : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

[132] Voir à ce sujet l'excellent article de T. LEONARD, *E-commerce et protection des données à caractère personnel : Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet*, disponible sur *http://www.droit.fundp.ac.be /Textes/Leonard1.pdf*

[133] En d'autres termes, nous soutenons que le placement d'un numéro identifiant dans un terminal de télécommunication ou le simple accès à ce numéro ou à un

AIDC, VOLUME XVII, *Droit constitutionnel et vie privée, Tunis 2007*

Conclusions de la troisième partie[134]

62. Le contexte de l'Internet couplé à celui des technologies de l'intelligence ambiante appelle une troisième génération de réglementations en matière de protection des données. Il ne s'agit pas de tourner le dos aux deux premières générations mais d'ajouter à celles-ci tout en ne modifiant pas les options déjà prises un niveau supplémentaire de protection. La première génération était essentiellement caractérisée par une approche fondée sur la nature de la donnée : était-elle sensible ? Appartenait-elle à la sphère intime de la personne concernée ? L'autodétermination informationnelle est alors comprise comme l'interdiction de traiter certaines données. C'est l'époque de la consécration de l'article 8 de la Convention européenne des droits de l'homme. La deuxième génération ajoute à la première la nécessité, au-delà de la protection de ces données particulières, d'envisager la façon dont le traitement de données à caractère personnel peut modifier les relations de pouvoir entre celui qui traite les données et celui à propos duquel le traitement a lieu. L'"autodétermination informationnelle" suppose la nécessité de rééquilibrer la relation en garantissant la transparence des traitements et en limitant le droit de traiter les données d'autrui. La Convention n° 108 est née dans cet esprit. Elle a fait de nombreuses émules et démontré ainsi amplement son bien-fondé. Cette approche européenne se caractérise par quelques éléments qui témoignent de l'enjeu public des questions de protection des données même lorsqu'il s'agit de relations entre personnes privées. Le consentement et l'autorégulation trouvent dans ce contexte leurs limites et l'autorité de contrôle indépendante créée par les pouvoirs publics, sa justification. Cette approche européenne aboutit avec la Charte européenne des droits de l'homme à la reconnaissance d'un droit constitutionnel à la protection des données, distinct de celui à la vie privée.

Ce qui caractérise la troisième génération que nous voyons poindre et dont nous souhaitons la consécration rapide est la prise en compte du fait technologique en lui-même. Que l'utilisation de la technologie multiplie

autre identifiant du terminal constituent un accès majoritairement non autorisé. Il n'importe pas, dans ce cadre légal, de jauger la proportionnalité de tels procédés. L'autorisation demeure un acte positif qui se distingue de l'acceptation qui peut se déduire d'un silence éventuel ou de l'absence d'opposition.

[134] Ces conclusions s'inspirent grandement des conclusions du rapport que l'auteur et J. –M. DINANT ont écrit pour le Conseil de l'Europe : *L'autodétermination informationnelle à l'ère de l'Internet, Eléments de réflexion sur la Convention n° 108 destineé au travail futur du Comité consultatif (T-PD),* voir note 6 supra, p. 385.

les données et les personnes capables d'y accéder, qu'elle accroît la puissance de ceux qui, grâce à cette technologie, peuvent les collecter et mieux les traiter, qu'elle abolisse les frontières est un premier constat. La complexité du fait technologique, son opacité constituent une seconde réalité à prendre en compte. Entre la personne concernée et les maîtres du fichier s'invite un troisième personnage tour à tour "terminal" et "réseau". L'autodétermination informationnelle passe dorénavant par une maîtrise de ce troisième personnage.

63. Comment envisager cette maîtrise ? Nous présentons ci-après quelques pistes de réflexion sans prétendre épuiser le sujet. La première concerne la façon d'y répondre. "The answer to the machine is in the machine" : cette affirmation, lancée par C. Clarke[135] à propos des problèmes rencontrés par la protection des droits d'auteur dans la société de l'information, peut servir de guide pour trouver une réponse adéquate aux risques encourus par la vie privée du fait de la société de l'information. Ainsi, nous avons vu que le principe de réciprocité des avantages, la promotion de solutions technologiques "Privacy Minded" peuvent favoriser une meilleure maîtrise par la personne concernée de la circulation et de l'utilisation de son image informationnelle.

Cet optimisme a des limites : si les technologies peuvent renforcer ce que certains appellent l'"User Empowerment", c'est au risque de laisser seule la personne concernée face au(x) maîtres du fichier. Ce risque est d'autant plus réel que le développement de la technologie n'est pas neutre : si la technologie de l'internet demeure largement "offerte" aux citoyens, son développement est financé de manière indirecte par les entreprises et les administrations qui paient les ordinateurs serveurs. De manière inéluctable, son développement penche donc tout naturellement du côté des intérêts des "ficheurs" plutôt que vers la défense des "fichés". La technologie dite de protection de la vie privée transforme ou risque de transformer la relation de l'individu à la donnée qui le concerne en une relation de propriété que la technologie permet de négocier. C'est le lieu de rappeler que l'autodétermination informationnelle est une liberté qui ne peut totalement se négocier et que c'est le devoir de la société de fixer certaines limites au droit de disposer de ces données. Il en va de la dignité humaine.

[135] C. CLARKE, "The answer to the machine is in the machine", in *The future of Copyright in a digital Environment,* B. HUGENHOLTZ (ed.), Kluwer, 1996, pp. 139 et ss.

64. Cette focalisation sur les outils technologiques doit amener à la prise en considération de nouveaux acteurs, non aperçus par les législations de deuxième génération : ainsi les fournisseurs de services de communication et les fournisseurs d'équipements terminaux. Leur rôle est décisif si on souhaite que l'utilisateur des services nouveaux de la société de l'information puisse contrôler les flux entrant et sortant de même que les traces laissées au fil des réseaux et leur possible utilisation. La responsabilité objective dans la fourniture d'équipements ou de services "privacy compliant" doit être envisagée.

En premier lieu, les fournisseurs d'accès à Internet, les opérateurs de mobilophonie ou de téléphonie se voient confiés la charge de sensibiliser le public sur les risques encourus lors de l'utilisation de leurs réseaux, de dénoncer les technologies "privacides" et, en même temps, de fournir un accès à des technologies "privaphiles" appropriées. Le rôle de ces fournisseurs d'accès est essentiel dans la mesure où ceux-ci représentent le point de passage obligé entre l'internaute et le réseau. Ainsi, leur demandera-t-on[136] d'"informer l'internaute des moyens techniques qu'il peut utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications", d'utiliser les procédures appropriées et les technologies disponibles, de préférence celles faisant l'objet d'une certification, garantissant la vie privée et notamment l'intégrité et la confidentialité des données ainsi que la sécurité physique et logique du réseau ...", "d'informer ces derniers (les internautes) des moyens d'utiliser ses services et de les payer anonymement". Il offrira à ses abonnés une hotline leur permettant de dénoncer des violations de la vie privée et souscrira à un code de conduite suivant lequel il bloquera l'accès aux sites qui ne respectent pas les exigences posées en matière de protection des données et ce, peu importe la localisation du site.

65. En second lieu, on vise les constructeurs et développeurs des matériels et logiciels qui conçoivent et construisent les équipements terminaux, ainsi que les responsables de l'élaboration des protocoles et des standards techniques utilisés pour transmettre des informations en réseau. Ils veilleront à concevoir des produits ou normes[137] :

- conformes, au cadre légal, par exemple par la transmission par les navigateurs internet des informations minimales nécessaires à la connexion ou par l'adoption de mesures de sécurité adéquates ;

[136] Recommandation n° R (99)5, point III ; 1, 2 et 4.

[137] *Cf.* à ce propos, l'avis de la Commission belge n° 34/2000 à propos de la protection des données dans le cadre du commerce électronique.

- qui facilitent l'application des principes dégagés ci-dessus au titre II et qui permettent par exemple un accès direct par l'utilisateur à ses données personnelles ou un droit d'opposition automatique, notamment par le biais de journaux de bord ;

- et qui améliorent le niveau de protection des données à caractère personnel.

L'outil technologique permet de plus en plus de traiter les données relatives à la personne concernée non point, comme c'était le cas de manière classique, par ses données d'identité légale (nom prénom, résidence, etc.) mais par un point d'ancrage voire par un objet (l'intelligence dite ambiante) qui lui est associé. Au-delà, le danger n'est souvent plus dans la collecte *a priori* de données sur l'individu mais sur l'application *a posteriori* à un individu d'un profil abstrait ...

Le terminal, conçu au sens large, doit être traité comme un outil technologique totalement transparent pour celui qui en est le détenteur et l'utilise. Mieux, dans de nombreux cas, il appartient à la personne concernée et pourrait être assimilé à son domicile, c'est-à-dire au lieu où la personne se sent chez elle. L'intrusion dans ce domicile privé doit être traitée comme toute autre intrusion.

L'opacité et la complexité des systèmes complexes d'informations auxquels les personnes concernées confient leurs données obligent à un surcroît d'informations non plus centrées sur le ou les traitements eux-mêmes pris séparément et sur leurs caractéristiques mais sur le fonctionnement global du système d'informations en tant que capable de générer une multitude de traitements présents ou à venir : ainsi, l'obligation de documenter les données (origine, utilisateurs, logique de raisonnement), d'établir un descriptif des circuits d'information) et de fixer les règles par lesquelles les décisions sont prises, les règles d'accès définies et contrôlées, etc.

66. La prise en considération de l'outil technologique a jusqu'à présent peu été le fait de ceux qui ont à garantir la protection des données : les autorités de protection des données disposent rarement d'une équipe d'informaticiens à même de décrypter les dangers des innovations technologiques. Sans doute serait-il utile de créer à l'échelon européen une "Privacy Technology Task Force" permanente, qui pourrait procéder à un Technology Assessment des solutions ou applications technologiques nouvelles ou émergentes. Par ailleurs, les autorités de protection des données se doivent de pénétrer les cénacles où se décident les évolutions technologiques et la configuration des produits. Ainsi, un dialogue avec

les organes de standardisation devrait être instauré[138] et sans doute au-delà, faudrait-il que le Governmental Advisory Committee (GAC) créé à l'initiative européenne auprès de l'ICANN, autorité privée qui décide de la gouvernance de l'Internet en matière d'adresses et de noms de domaines se penche sur la question de la protection des données. On peut suggérer voire imposer la création d'un "Data Protection Advisory Committee" auprès de l'ICANN, du W3C et de l'IETF ?

La sensibilisation du milieu sectoriel de la communication électronique aux enjeux de protection des données s'avère en tout cas nécessaire.

67. En conclusion, les diverses pistes proposées ont pour objectifs :

- de mettre à la disposition de l'individu tout ce qui est nécessaire pour comprendre et maîtriser son environnement informationnel en particulier celui qui pénètre son foyer. Il lui donne la maîtrise des outils dont l'utilisation le révèle à autrui ;

- de confier à la société les outils lui permettant de pouvoir continuer à maîtriser un développement technologique, dont l'enjeu est bien la survie de nos libertés tant individuelles que collectives.

Sur le réseau routier, la législation a imposé certaines règles à ses usagers afin, non seulement d'éviter des accidents, mais bien aussi de régler de manière équitable les droits et obligations réciproques des différents usagers de la route, avec en général, une propension prétorienne à protéger tout naturellement l'usager le plus faible. Pour ce faire, au-delà du code

[138] A ce propos les démarches opérées par le groupe dit de l'article 29 et relatées in Note d'information générale concernant le rapport du CEN/ISSS sur la normalisation au service de la protection de la vie privée en Europe (CEN, Centre européen de normalisation) (Avis 1/2002),30 mai 2002, note disponible sur le site de la Commission déjà cité et surtout la résolution prise à Wroclaw lors de la 26ème conférence internationale de protection de la vie privée et des données à caractère personnel qui consacre les efforts de l'ISO en la matière : "Whereas the International Working Group on Data Protection in Telecommunications at their 35th meeting in Buenos Aires on 14-15 April 2004 has adopted a Working Paper on a future ISO Privacy Standard ;"

"Whereas the International Conference of Data Protection and Privacy Commissioners (hereafter "Conference") wishes to support the development of an effective and universally accepted international privacy technology standard and make available to ISO its expertise for the development of such a standard ; ..."

Sur le thème : "standardisation et vie privée", on lira P. ROSENSWEIG et A.KOCHEMS, "Data Protection : Safeguarding Privacy in a New Age of Technology", 23 mars 2005 publié in *http://www.heritage.org/Research/HomelandDefense/lm16.cfm*

AIDC, Volume XVII, *Droit constitutionnel et vie privée*, Tunis 2008

AIDC, VOLUME XVII, *Droit constitutionnel et vie privée*, Tunis 2007

de la route, est apparue la nécessité d'une intervention législative toute particulière afin de réglementer le réseau routier lui-même ainsi que les véhicules qui sont admis à y circuler, moyennant le respect de certaines normes obligatoires.

Sur les autoroutes de l'information, il n'existe aucune législation qui s'attache à définir des normes de fonctionnement des télécommunications respectueuses de la protection de la vie privée des internautes ou encore des exigences de fonctionnement loyal et transparent des terminaux de télécommunication permettant aux internautes de circuler sur ces autoroutes.

Ce n'est pourtant qu'en appliquant les principes classiques de la protection des données à la technologie, ce troisième larron qui s'invite de manière implicite mais certaine dans toute télécommunication, que l'informatisation de la société pourra conduire à une société de l'information démocratique, moteur de progrès partout et pour tous.

CONCLUSIONS GÉNÉRALES ET PERSPECTIVES LE DROIT DE LA PROTECTION DES DONNÉES, UN DROIT EN MARCHE

68. La jurisprudence du Conseil de l'Europe déduit de l'article 8 de la Convention européenne des droits de l'homme non seulement une obligation négative de ne pas interférer avec la vie privée des citoyens mais en outre des obligations positives de l'État de mettre à disposition des citoyens les moyens de pouvoir exercer pleinement les prérogatives liées au respect de cette autonomie et des diverses facettes de cette autonomie tant dans les relations du citoyen avec l'État mais également dans la relation qu'il entretient avec les autres citoyens (effet dit horizontal de la CEDH[139]). La Cour de Strasbourg se réserve le droit d'examiner si l'État, par omission ou par action, a maintenu un "juste équilibre" entre, d'une part, l'intérêt général, les différents droits et intérêts en présence et, d'autre part, l'intérêt de l'individu à la protection de sa vie privée entendue au sens le plus large[140].

[139] Sur cette "horizontalisation" des droits de l'Homme et en particulier de la vie privée, lire S. VANDROOGHENBOECK, "L'horizontalisation" des droits de l'homme", *in* H. DUMONT et alii (ed.), *La responsabilité, face cachée des droits de l'homme*, Bruxelles, Bruylant, 2005, pp. 355 à 390,

[140] Sur cet équilibre entre droits, libertés et intérêts, lire Y. POULLET, "La protection des données, entre libertés, droits subjectifs et intérêts légitimes", *in Liber Amicorum P. Martens,* Bruxelles, Larcier, 2007, pp. 133 à 150.

69. C'est précisément au vu de cette obligation positive de l'État que l'irruption du fait technologique a rendu nécessaire l'intervention législative des États en matière de protection des données à caractère personnel. L'utilisation de plus en plus massive de données à caractère personnel et leur traitement par des outils logiciels de plus en plus performants constituent des risques nouveaux pour l'autodétermination de chacun. On note la réduction de chacun à ses données et dès lors au profil que ces données dessinent, qui crée le risque de discrimination ou simplement d'erreur. On ajoute le déséquilibre informationnel que les traitements des entreprises, des associations et des administrations entretiennent entre ces derniers et la personne concernée. On souligne enfin l'opacité des traitements et en tout cas des raisonnements à l'œuvre derrière ces traitements, qui crée le risque d'un "conformisme anticipatif" dénoncé dès 1983 par le tribunal constitutionnel allemand de Karlsruhe, qui conduit chacun à se modeler suivant la norme de comportement accepté par la majorité. Tous ces éléments empêchent les personnes de participer pleinement à la vie sociale et d'y apporter leur contribution originale. La Convention n° 108 du Conseil de l'Europe relaie cette préoccupation en faisant "peser une responsabilité sociale accrue sur les acteurs publics et privés"[141] et en affirmant les principes de transparence, de proportionnalité et de sécurité comme fondement même des initiatives législatives en la matière. Il s'agit à travers ces législations de créer un certain droit de contrôle individuel et collectif sur la circulation de l'image informationnelle. En d'autres termes, les législations de protection des données apparaissent comme un "moyen" dérivé du droit à la vie privée, pour assurer la protection des valeurs éthiques de dignité et d'autonomie personnelle et ce dans un contexte donné : celui du développement des technologies de l'information et de la communication

70. Les écrits de LESSIG[142] et de REIDENBERG[143] parmi d'autres attirent notre attention sur la nécessité de tenir compte dans la reconnaissance de la Privacy de l'architecture du système dans lequel nous évoluons et sur-

[141] Rapport explicatif de la Convention n° 108.

[142] L. LESSIG, *Code and other Laws of Cyberspace*, Basic Books, New York, 1999. Sur ces relations entre Droit et Technologie, lire nos réflexions *in Mélanges G. HORSMANS,* Bruylant, 2004, pp. 942 et s. Plus récemment la thèse de E. LABBE, *Les équilibres juridiques à l'épreuve de la contrainte technique. Conflits et défis normatifs de la société de l'information,* thèse dactylographiée, Montréal, 2 tomes, Juin 2006.

[143] J. REIDENBERG, "Lex informatica. The Formulation of information Policy through Technology", *Emory Law Journal,* 1996, pp. 911 et s.

tout de son évolution. Les règles affirmées dans une société où les traitements de l'information nominative venaient de voir le jour doivent donc être réévaluées aujourd'hui à l'aune de la dimension ubiquitaire, globale et interactive de nos réseaux et des systèmes d'intelligence ambiante. Ainsi à l'heure où la technologie est ubiquitaire, trace chacun de nos gestes et choix fussent-ils les plus instantanés et pénètre nos foyers, il est important que de nouveaux droits soient affirmés : celui d'une protection de la "virtual home" au-delà de la "physical home", celui de la maîtrise et de la transparence de nos terminaux, le droit de se déconnecter et d'utiliser un pseudonyme dans nos communications avec autrui.

Le droit de s'opposer aux communications non sollicitées participe également de ce même souci de ne pas être victimes d'intrusions et d'être laissé seul. Par ailleurs, ce droit s'explique également par la volonté de ne pas être réduit à son profil et confirmé dans celui-ci, sans pouvoir être surpris et invité au changement.

71. Certains de nos gestes parce qu'ils sont triviaux ou parce qu'ils répondent à une sollicitation instantanée sont conçus comme ne laissant pas de traces (si ce ne sont celles recueillies éphémèrement ou non, consciemment ou non par un voisin). La technologie actuelle permet de collecter ces informations, de les traiter et d'en déduire, connectées ou non à d'autres informations, des profils de personnalité permettant d'agir vis-à-vis des personnes concernées. Par leur enregistrement et leur conservation, les traces précédemment volatiles de nos activités et comportements les plus anodins revêtent à présent du sens, dans la mesure où elles sont interprétés, seules ou en relation avec d'autres traces tout aussi anodines par elles-mêmes mais néanmoins enregistrées. Les individus n'ont le plus souvent aucun contrôle sur le sens qui est ainsi produit, sur la construction du "savoir" qui pourtant les concerne. Ils n'ont d'ailleurs que très peu conscience de l'existence de ces constructions et leurs "expectations of privacy", notamment en ce qui concerne des gestes et comportements auxquels eux-mêmes n'attachent aucune signification. Dans le contexte de certains systèmes d'intelligence ambiante, les personnes se voient réduites à devenir, au sein des réseaux qui les entourent, un pur objet en relation avec d'autres objets qui interagissent à leur présence.

72. Si l'autodétermination n'est pas un droit purement égoïste mais une condition qui représente un élément structurant pour notre participation dans une société démocratique, l'approche en termes de propriété par le sujet de ses données à caractère personnel est à rejeter. De même, si le consentement peut à juste titre être considéré comme une des conditions nécessaires de légitimité des traitements, il ne peut comme l'affirme cer-

taines théories néolibérales (Posner-Epstein) être une cause suffisante de légitimité. Ce point est important dans la mesure où la technologie crée l'illusion en tout cas d'un possible "user empowerment" (PICS, P3P) où l'internaute serait lui-même apte à décider des traitements qu'il autorise. La doctrine du consentement comme fondement suffisant du traitement des données ne prend en compte ni la question des "capabilitiés"[144] dans la société de l'information, le fait que les nécessités ou avantages liés à la vente de données peuvent être attractifs pour des personnes fragiles socio-économiquement parlant, ni la théorie des dominos qui met en évidence le fait que la divulgation volontaire par une personne de "ses" données personnelles "force" les autres à donner la même information, sous peine de suspicions envers eux[145].

Par ailleurs, la technologie permet dans de nombreux secteurs de développer des mécanismes décisionnels "one-to-one" fondés sur l'accumulation de données qui permettent un profilage fin. Cette pratique pose deux questions. Premièrement, peut-on admettre la prise en considération de n'importe quelle donnée même si son utilisation dans une perspective de rationalité économique le justifie (exemple : la situation de femme battue dans le cadre du calcul d'une prime d'assurance-vie) ? Ne faut-il pas obliger les décideurs à mieux expliciter leurs critères de décision et permettre une négociation collective et le cas échéant arbitrée par une autorité sur la proportionnalité de ces systèmes ? Seconde question, il est important de rappeler aujourd'hui le principe de la compatibilité des traitements, fondés en définitive sur la question de l'intégrité contextuelle[146], la personne donne son information dans un contexte donné et s'attend raisonnablement qu'elle soit traitée dans ce contexte, sous peine de risquer d'être jugée "hors contexte".

73. Le caractère global de nos réseaux et l'importance des risques encourus par nos autonomies du fait même des technologies à l'œuvre au sein de ces réseaux amènent à prôner une reconnaissance globale des règles de protection des données. Lors de sa réunion de Tunis, le Sommet mondial de la société de l'information a appelé de ses vœux la définition d'une charte globale en matière de Privacy devant trouver dans des modes divers de régulation adaptés à chaque culture son expression. La convention n° 108 pourrait apparaître, sur le modèle de la Convention sur la cybercriminalité ouverte avec succès à des pays non-membres du Conseil de l'Europe, comme la base sur laquelle pourrait se construire ce consensus mondial.

[144] Voir Amartya Sen, *Inequality Reexamined*, Harvard University Press, 1995.

[145] Margaret Jane RADIN, "Justice and the Market Domain", *in* John CHAPMAN, J. Roland PENNOCK, *Markets and Justice*, New York University Press, 1989, p. 168. : " the domino theory asserts that market evaluations of objects and activities are imperialistic, diving out other and better ways of perceiving and evaluating objects and activities. Once some individuals attach a price at a given object, relation or activity, they and others tend to lose their capacity to perceive or evaluate that object, relation or activity as anything but a commodity with a specific market price. Moreover, the theory asserts, once certain objects or activities are commodified, there is a tendency for other objects or activities of the same sort or even of other sorts also to be seen and evaluated merely in terms of their actual or potential market value." Pour une exploration plus détaillée de ce theme voir Antoinette ROUVROY, "Information génétique et assurance. Discussion critique autour de la position "prohibitionniste" du législateur belge", *JT* n° 5978, 2000, 585-603 et Antoinette ROUVROY, *Human Genes and Neoliberal Governance : A Foucauldian Critique*, Routledge-Cavendish, 2007, (Chapter 7 : A critical assessment of economic and actuarial perspectives on genetics and insurance).

[146] H. NISSENBAUM, "Privacy as Contextual Integrity" *Washington Law Review*, vol. 79, n. 1, February 4, 2004. 119-158).